



BiPAC 7800GZ(L)

**3G/ 802.11g ADSL2+ (VPN) Firewall
Router**

User Manual

Table of Contents

Chapter 1: Introduction	1
Introduction to your Router	1
3G Mobility and Always-On Connection	1
Secure VPN Connections (BiPAC 7800GZ only)	1
Smooth, Responsive Net Connection	1
Wireless Mobility and Double-layer Protection	2
Features	3
ADSL Compliance	3
3G/HSPA	3
Network Protocols and Features	4
Virtual Private Network (VPN) (BiPAC 7800GZ only)	4
Firewall	4
Quality of Service Control	4
IPTV Applications	5
ATM and PPP Protocols	5
Wireless LAN	5
Management	6
Hardware Specifications	6
Physical Interface	6
Chapter 2: Installing the Router	7
Package Contents	7
Important note for using this router	8
Device Description	9
The Front LEDs	9
The Rear Ports	10
Cabling	11
Chapter 3: Basic Installation	12
Connecting Your Router	13
Network Configuration	15
Configuring PC in windows 7	15
Configuring PC in Windows Vista	17
Configuring PC in Windows XP	19
Configuring PC in Windows 2000	20
Configuring PC in Windows 95/98/Me	21
Configuring PC in Windows NT4.0	22
Factory Default Settings	23
Information from your ISP	25
Chapter 4: Configuration	26
Easy Sign-On (EZSO)	26
Configuration via Web Interface	29
Quick Start	30
Basic Configuration Mode	47
Status	47
WAN – Main Port (ADSL)	48
PPPoE Connection (ADSL)	48
PPPoA Connection (ADSL)	49
MPoA Connection (ADSL)	50
IPoA Connections (ADSL)	51
Pure Bridge Connections (ADSL)	52
WAN – Main Port (EWAN)	53
PPPoE (EWAN)	53
Obtain IP Address Automatically (EWAN)	54

Fixed IP Address (EWAN)	54
Pure Bridge (EWAN)	55
WAN – Main Port (3G)	55
WLAN	57
Advanced Configuration Mode	61
Status	61
ADSL Status	62
WAN Statistics	63
3G Status	64
ARP Table	65
DHCP Table	66
System Log	67
Firewall Log	68
UPnP Portmap	68
IPSec Status	69
VRRP Status	69
Configuration	70
LAN - Local Area Network	71
Ethernet	71
IP Alias	71
Wireless	72
Wireless Security	75
WPS	79
DHCP Server	92
VRRP	94
WAN - Wide Area Network	95
WAN Interface	95
WAN Profile	98
Mobile Networks	110
ADSL Mode	111
System	112
Time Zone	112
Firmware Upgrade	113
Backup / Restore	114
Restart	115
User Management	116
Mail Alert	117
SMS Alert	119
Syslog	120
Diagnostics Tools	120
Firewall	121
Packet Filter	121
Ethernet MAC Filter	125
Wireless MAC Filter	126
Intrusion Detection	127
Block WAN Ping	128
URL Filter	129
VPN	131
IPSec	131
GRE	135
QoS - Quality of Service	136
Virtual Server	141
Port Mapping	143
DMZ	145
One-to-One NAT	146
ALG	147
Wake on LAN	148

Certificate.....	149
Trusted CA.....	149
Time Schedule	152
Advanced	153
Static Route	153
Static ARP	155
Static DNS	156
Dynamic DNS	157
VLAN	159
Device Management.....	162
IGMP	168
TR-069 Client.....	169
Remote Access.....	170
Web Access Control	171
Save Configuration to Flash	172
Restart.....	173
Logout.....	174
Chapter 5: Troubleshooting.....	175
Appendix: Product Support & Contact	177

Chapter 1: Introduction

Introduction to your Router

The BiPAC 7800GZ(L), a Dual-WAN 3G / ADSL2+ firewall router integrated with the 802.11g Wireless Access Point and 4-port switch is a cutting-edge networking product for SOHO and office users. Uniquely, the router offers users more flexibility to directly insert a 3G / HSPA SIM card into its built-in SIM slot instead of requiring external USB modems. This design will avoid compatibility issues of many different 3G USB modems. With the increasing popularity of the 3G standard, communication via the BiPAC 7800GZ(L) is becoming more convenient and widely available - enabling users to use a 3G / UMTS HSDPA / HSUPA or GSM GPRS / EDGE Internet connection, making downstream rates of up to 7.2Mbps possible. Users can watch movies, download music on the road or access e-mail wherever a 3G connection is available. Additionally, the integrated IPSec VPN function allows you to encrypt connections of up to 4 VPN tunnels to securely transmit data over the Internet (BiPAC 7800GZ only). The support for auto fail-over means that users will be assured of a constant Internet connection - in the event that the ADSL line fails, the BiPAC 7800GZ(L) will connect via the embedded 3G card to deliver uninterrupted connectivity.

3G Mobility and Always-On Connection

The BiPAC 7800GZ(L) router allows you to insert a 3G / HSPA USIM card to its built-in SIM slot, enabling you to use a 3G / HSPA, UMTS, EDGE, GPRS, or GSM Internet connection, which makes downstream rates of up to 7.2Mbps^{*4} possible. With the increasing popularity of the 3G standard, communication via the BiPAC 7800GZ(L) is becoming more convenient and widely available - allowing you to watch movies, download music on the road, or access e-mail no matter where you are. You can even share your Internet connection with others, no matter if you're in a meeting, or speeding across the country on a train. The auto fail-over feature ensures maximum connectivity and minimum interruption by quickly and smoothly connecting to a 3G network in the event that your ADSL line fails. The 7800GZ(L) will then automatically reconnect to the ADSL connection when it's restored, reducing connection costs. These features are perfect for office situations where constant connection is paramount.

Secure VPN Connections (BiPAC 7800GZ only)

The BiPAC 7800GZ supports embedded IPSec VPN (Virtual Private Network) protocols, allowing users to establish encrypted private connections of up to 4 simultaneous tunnels over the Internet. So that you can access your corporate intranet and transmit sensitive data between branch offices and remote sites anytime; even when you are on the road, thus enhancing productivity

Smooth, Responsive Net Connection

Quality of Service (QoS) gives user full control over outgoing data traffic. Priority can be assigned by the router to ensure that important transmissions like gaming packets, VoIP calls or IPTV / streaming content passes through the router at lightning speed, even when there is heavy Internet traffic. The speed of different types of outgoing data passing through the router is also controlled to ensure that users do not saturate bandwidth with their browsing activities.

Wireless Mobility and Double-layer Protection

An integrated 802.11g Wireless Access Point offers quick yet easy access with data encryption for added security. Wi-Fi Protected Access (WPA-PSK / WPA2-PSK) and Wired Equivalent Privacy (WEP) support ensures high-level data protection and WLAN access control. In addition, rich firewall security features such as SPI, DoS attack prevention and URL content filtering are integrated to provide unparalleled protection for Internet access. The router also supports the Wi-Fi Protected Setup (WPS) standard, allowing users to establish a secure wireless network by simply pushing a button. If your network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function allows you to expand your wireless network without the need for any external wires or cables.

Features

- Dual WAN approach - ADSL2+, 3G or Ethernet WAN for broadband connectivity.
- 3G/ HSPA embedded with a built-in SIM card slot
- Integrated 4-port Ethernet switch, one port can be configured as a WAN interface
- 4 IPSec VPN tunnels supported (BiPAC 7800GZ only)
- 4 GRE VPN tunnels supported (BiPAC 7800GZ only)
- Secure VPN with powerful DES / 3DES / AES (BiPAC 7800GZ only)
- High-speed Internet access via ADSL2 / 2+; backward compatible with ADSL
- Supports 802.11g wireless access point with WPA-PSK / WPA2-PSK
- WPS (Wi-Fi Protected Setup) for easy setup
- Quality of Service control for traffic prioritization and bandwidth management
- SOHO firewall security with DoS prevention and Packet Filtering
- Supports IPTV application^{*2}

ADSL Compliance

- Compliant with ADSL Standard
- Full-rate ANSI T1.413 Issue 2
- G.dmt (ITU G.992.1)
- G.lite (ITU G.992.2)
- G.hs (ITU G.994.1)
- ADSL over ISDN / U-R2
- Compliant with ADSL2 Standard^{*1}
- G.dmt.bis (ITU G.992.3)
- ADSL2 Annex M (ITU G.992.3 Annex M) (BiPAC 7800GZA only)
- Compliant with ADSL2+ Standard^{*1}
- G.dmt.bis plus (ITU G.992.5)
- ADSL2+ Annex M (ITU G.992.5 Annex M) (BiPAC 7800GZA only)

3G/HSPA^{*4}

- Supports third generation (3G/ 3.5G/ 3.75G) digital cellular standards
- Peak downlink speeds up to 7.2Mbps and peak uplink speeds up to 2.0Mbps
- Web-based GUI for 3G configuration and management

Network Protocols and Features

- NAT, static routing and RIP-1 / 2
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server and DMZ
- SNTP, DNS relay and IGMP Proxy
- IGMP snooping for video service
- Management based-on IP protocol, port number and address
- SMTP client with SSL/TLS

Virtual Private Network (VPN) (BiPAC 7800GZ only)

- 4 IPSec VPN Tunnels
- 4 GRE VPN Tunnels
- IKE key management
- DES, 3DES and AES encryption for IPSec.
- IPSec pass-through

Firewall

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- Prevents DoS attacks including Land Attack, Ping of Death, etc.
- Remote access control for web base access
- Packet Filtering - port, source IP address, destination IP address, MAC address
- URL Content Filtering - string or domain name detection in URL string
- MAC Filtering
- Password protection for system management
- VPN pass-through

Quality of Service Control

- Supports the DiffServ approach
- Traffic prioritization and bandwidth management based-on IP protocol, port number and address

IPTV Applications^{*2}

- IGMP Snooping
- Virtual LAN (VLAN)
- Quality of Service (QoS)
- IGMP Snooping & IGMP Proxy

ATM and PPP Protocols

- ATM Adaptation Layer Type 5 (AAL5)
- Multiple Protocol over AAL5 (RFC 2684, formerly RFC 1483)
- Bridged or routed Ethernet encapsulation
- VC and LLC based multiplexing
- PPP over Ethernet (PPPoE)
- PPP over ATM (RFC 2364)
- Classical IP over ATM (RFC 1577)
- MAC Encapsulated Routing (RFC 1483 MER)
- OAM F4 / F5

Wireless LAN

- Compliant with IEEE 802.11g and 802.11b standards
- 2.4 GHz - 2.484 GHz frequency range
- Up to 54Mbps wireless operation rate
- Wi-Fi Protected Setup (WPS) for easy setup
- 64 / 128 bits WEP supported for encryption
- Wireless Security with WPA-PSK / WPA2-PSK supported
- WDS repeater function support
- 802.1x radius supported
- WLAN on/off time schedule control

Management

- Easy Sign-On (EZSO) and Auto-scan ADSL settings
- Web-based GUI for remote and local management
- Firmware upgrades and configuration data upload and download via web-based GUI
- Embedded Telnet server and SSH for remote and local management
- Available Syslog
- Mail Alert for WAN IP Changed, Failover indication
- Wake on LAN
- High availability (device redundancy)
- Supports DHCP server / client / relay
- TR-069^{*3} supports remote management
- SNMP v1/v2/v3^{*3} supports remote and local management



1. The router may require firmware modification for certain ADSL2 / 2+ / Annex M DSLAMs.
2. IPTV application may require subscription to IPTV services from a Telco / ISP.
3. Either TR-069 or SNMP v1/v2/v3 can be available; but only upon request for Telco / ISP tender projects. The TR-069 and SNMP v1/v2/v3 software can only be applied to one device and will not work together on the same device.
4. The 3G / HSDPA data rate is dependent on your local service provider and your 3G / HSDPA card.

Hardware Specifications

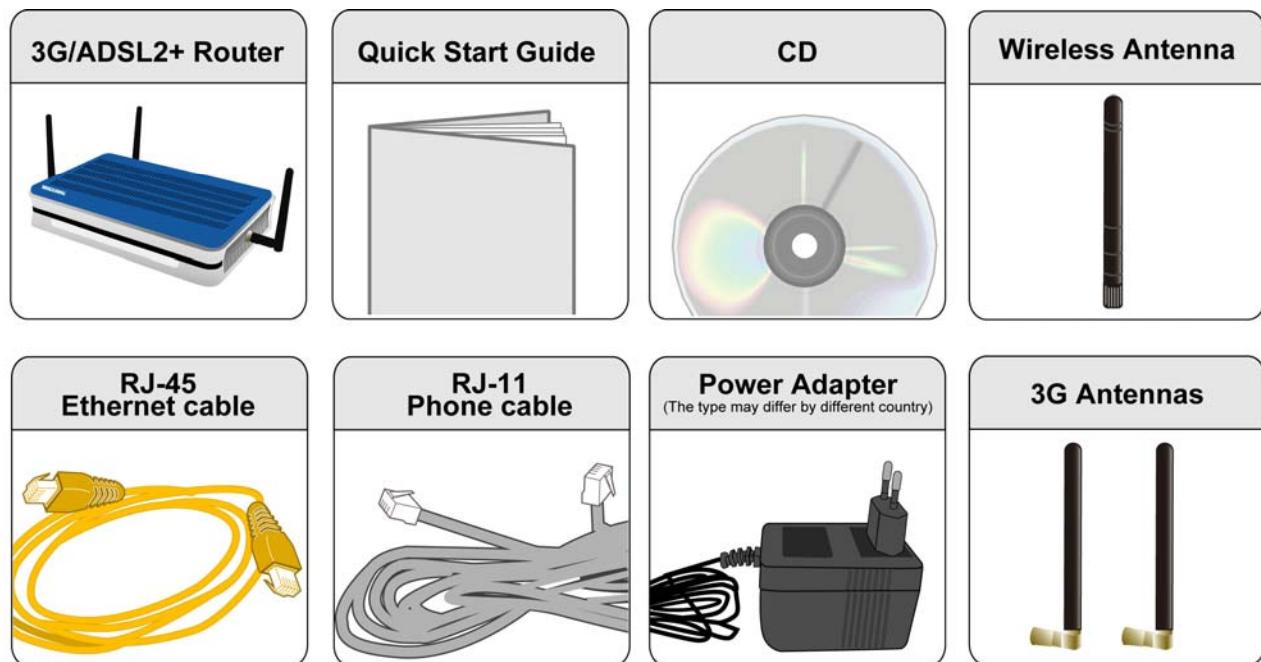
Physical Interface

- 3G wireless: 2pcs. x 3G antennae
- Power jack
- Power switch
- Factory default reset button
- WPS push button
- SIM slot: (for the SIM card from Telco / ISP)
- Ethernet: 4-port 10 / 100Mbps auto-crossover (MDI / MDI-X) Switch
- EWAN: Ethernet port #4 can be configured as a WAN interface for connecting to ADSL / Cable / VDSL / Fiber modem device
- DSL: ADSL port
- WLAN: 1pce x 2dBi detachable antenna

Chapter 2: Installing the Router

Package Contents

- 3G/ 802.11g ADSL2+ (VPN) Firewall Router
- CD containing the online manual
- RJ-11 ADSL/Telephone cable
- Ethernet (RJ-45) cable
- One 2dBi Wireless detachable antenna
- Two 3G antennas
- Power adapter
- Quick Start Guide
- Splitter / Micro-filter (Optional)



Important note for using this router



Warning

- Do not use the router in high humidity or high temperatures.
- Do not use the same power source for the router as other equipment.
- Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Avoid using this product and all accessories outdoors.

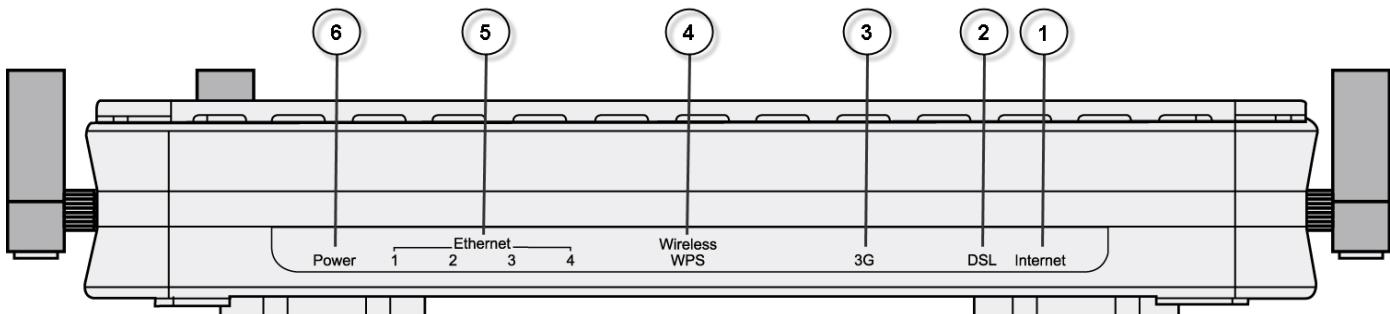


Attention

- Place the router on a stable surface.
- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

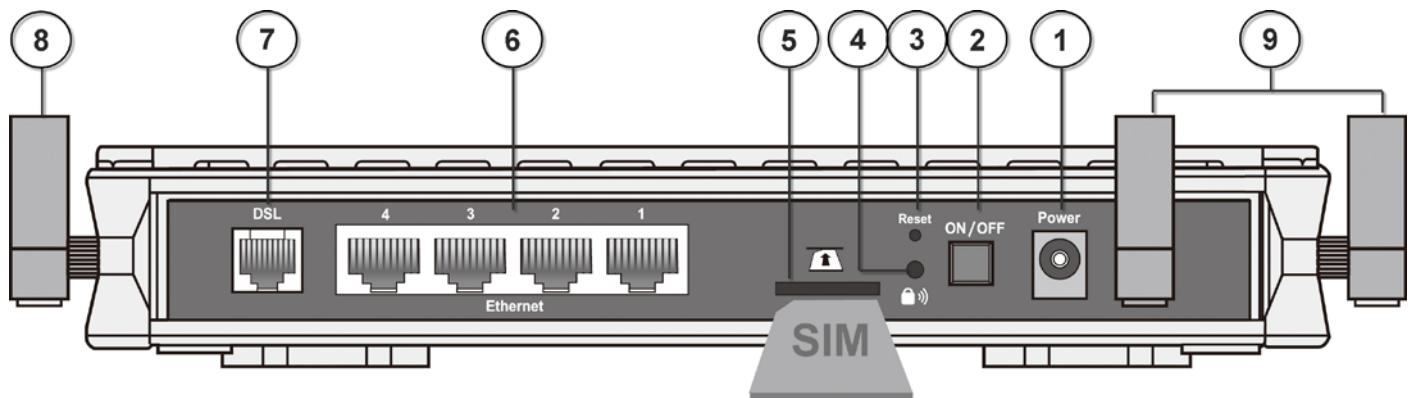
Device Description

The Front LEDs



LED		Meaning
1	Internet	<p>Lit red when WAN port fails to get IP address.</p> <p>Lit green when WAN port gets IP address successfully.</p> <p>Lit off when the device is in bridge mode or when ADSL connection is absent.</p>
2	DSL	Lit green when the device is successfully connected to an ADSL DSLAM. ("line sync")
3	3G	<p>Lit green when 3G service is ready.</p> <p>Blinking orange slowly when 3G signal is weak; blinking orange fast when 3G signal is middle; lit up orange steady when 3G signal is strong.</p> <p>Lit off when there is no 3G signal.</p>
4	Wireless / WPS	<p>Lit green when a wireless connection is established.</p> <p>Flash orange when WPS configuration is in progress. However, if WPS fails the LED will only lit for 1 min before goes off.</p> <p>Blinking when data is transmitted/received.</p>
5	Ethernet port 1X - 4X (RJ-45 connector)	<p>Lit green when successfully connected to an Ethernet device.</p> <p>Blinking when data is transmitted/received.</p>
6	Power	<p>When the device is booting, the green light will lit while the red light will flash.</p> <p>When the system is ready, it will lit green.</p> <p>Lit red when the device fails to boot or when the device is in emergency mode.</p>

The Rear Ports



Port	Meaning
1 Power	Connect it with the supplied power adapter.
2 Power Switch	Power ON/OFF switch.
3 Reset	Press for more than 5 seconds to restore the device to its default mode.
4 WPS	By controlling the pressing time, users can achieve two different effects: (1) <u>WPS</u> : Press less than 5 seconds until WPS LED flashes orange to trigger WPS function. But if WPS service is disabled, this short time press does nothing. (2) <u>Wireless ON/OFF button</u> : Press over 5 seconds to switch on wireless function and the Wireless/WPS LED will lit green. Press over 5 seconds again to disable wireless function and the Wireless/WPS LED is off.
5 USIM	Insert a SIM card into this slot. Warning: Before inserting or removing the SIM card, you must disconnect the router from the power adapter.
6 Ethernet	Connect your computer to a LAN port using the included Ethernet cable (with RJ-45 cable) Ethernet port 4 can be used for EWAN
7 DSL	Connect the supplied RJ-11 cable to this port when connecting to the ADSL/telephone network
8 Wireless Antenna	Connect the detachable antenna for wireless connection.
9 3G Antenna	Connect the detachable antennas to these two ports for 3G connection.



Connect the detachable 3G antennae to the two jacks on the back and right side of device(from the perspective of rear panel). Making sure they are firmly screwed in.

Cabling

One of the most common causes of problem is bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front panel of your router is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify if you are using the proper cables. If the error persists, you may have a hardware problem. In this case you should contact technical support.

Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.

Chapter 3: Basic Installation

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista, etc. The product provides an easy and user-friendly interface for configuration.

Please check your PC network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.1.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

Please follow the following steps to configure your PC network environment.

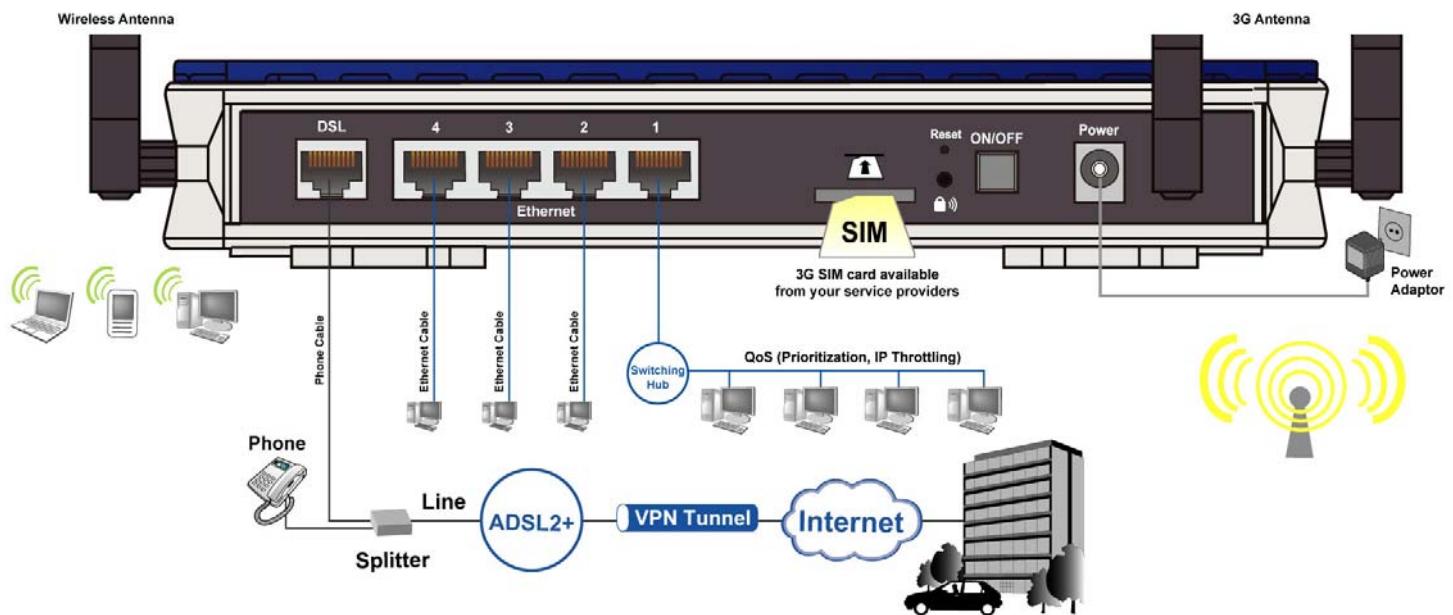


Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

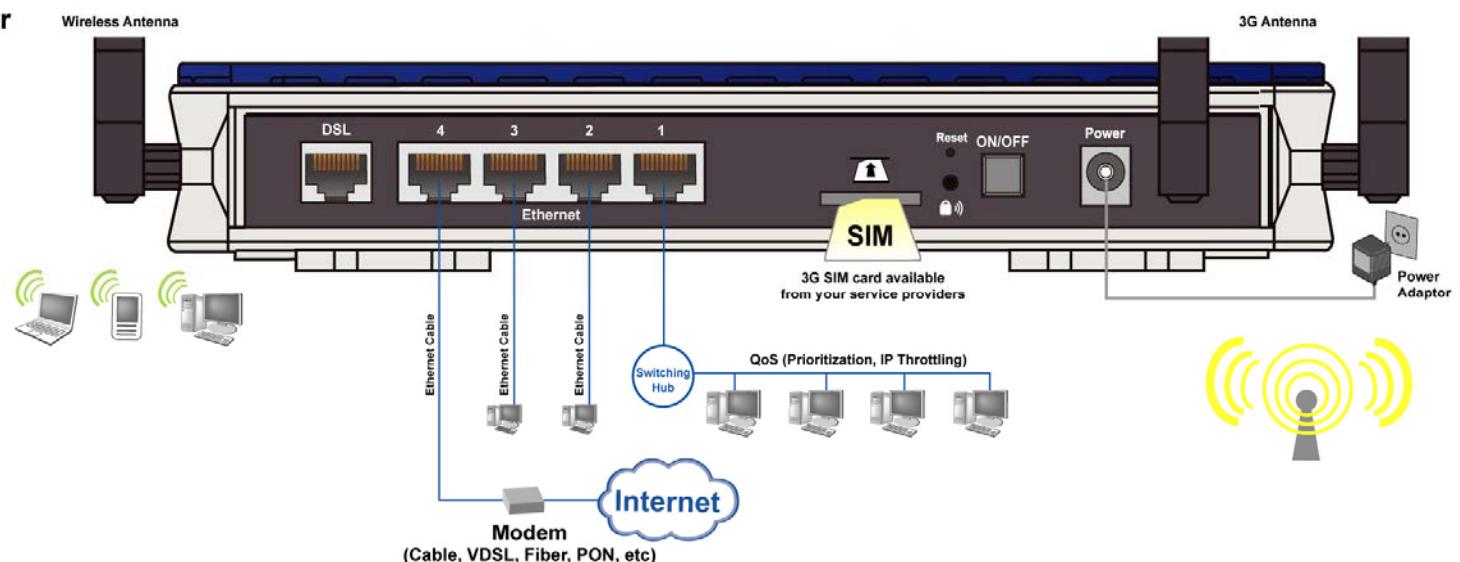
Connecting Your Router

BiPAC 7800GZ(L) offers three modes to connect to the internet. Besides using ADSL, users can set EWAN (Ethernet port # 4) or 3G for internet connection. BiPAC 7800GZ(L) also allows Dual WAN connection: ADSL fail-over to 3G, EWAN fail-over to 3G, ADSL fail-over to EWAN, and counter likewise.

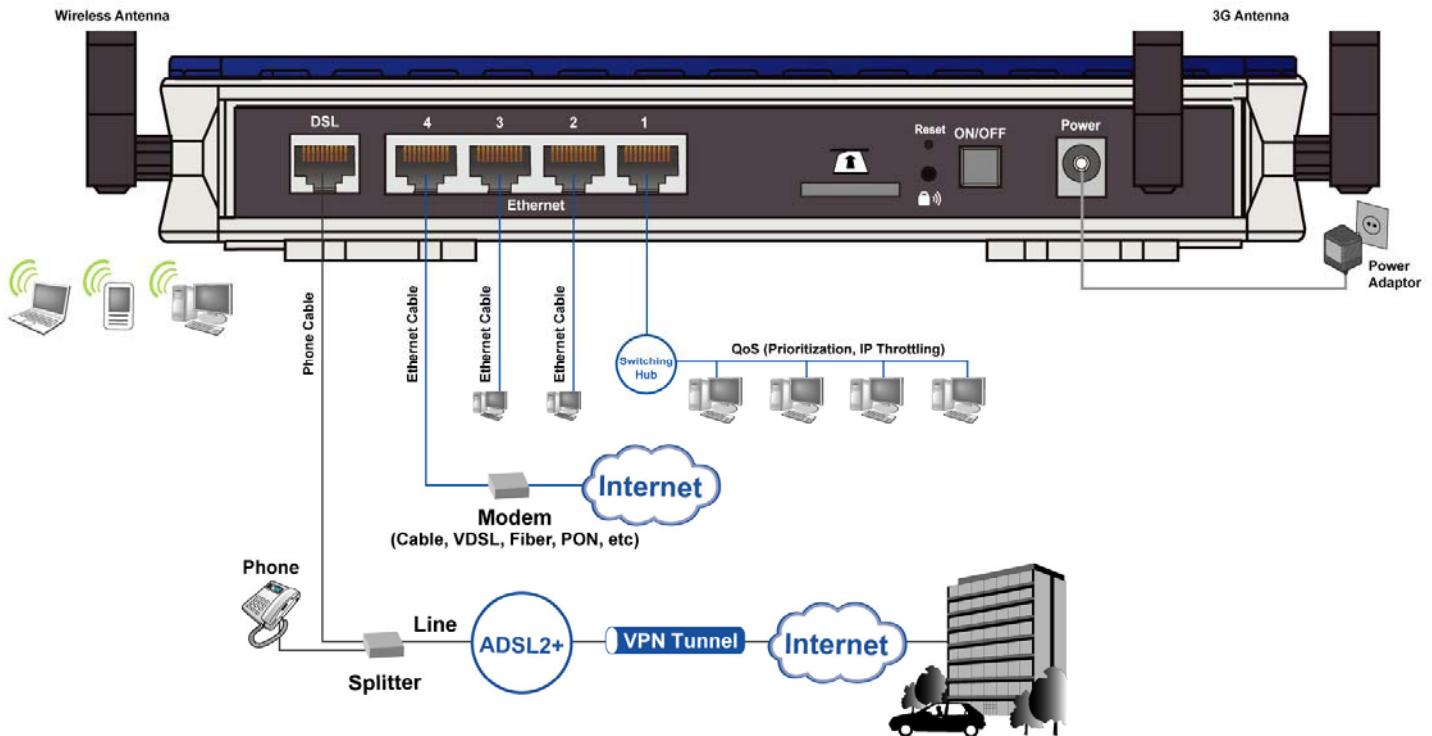
ADSL fail-over to 3G



Broadband (EWAN) fail-over to 3G



ADSL fail-over to EWAN

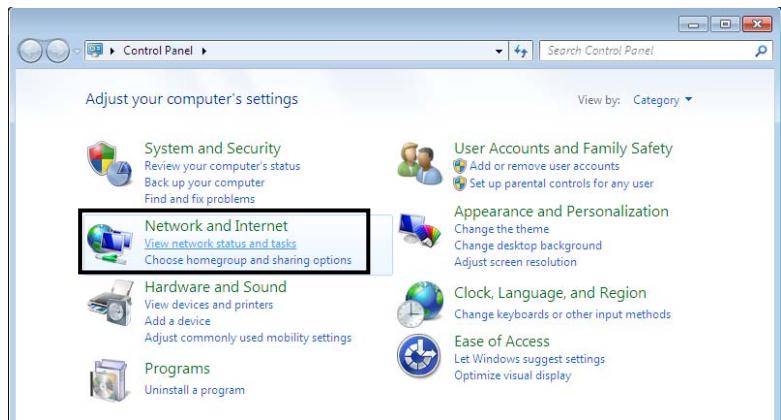


Network Configuration

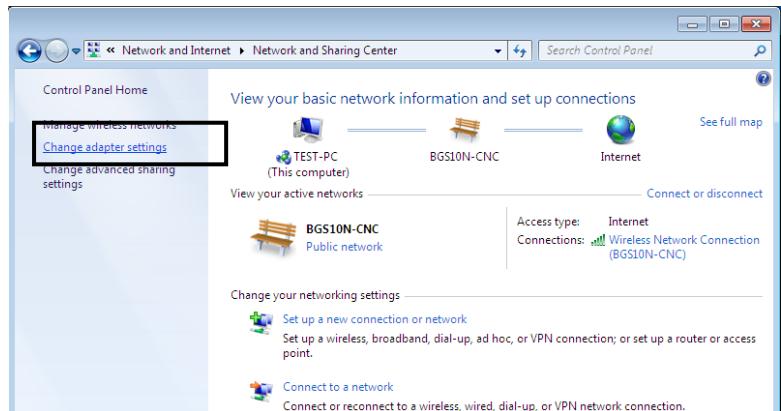
Configuring PC in windows 7

1. Go to Start. Click on Control Panel.

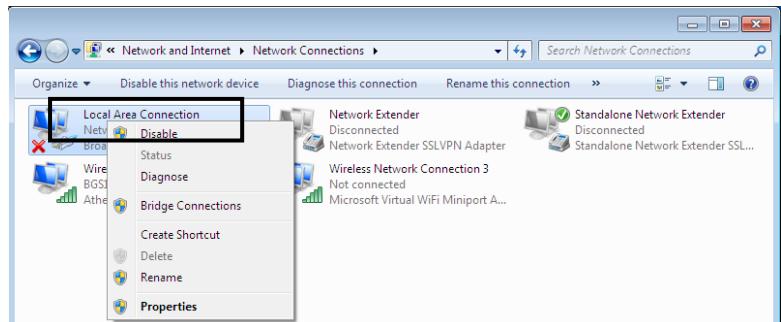
Then click on Network and Internet.



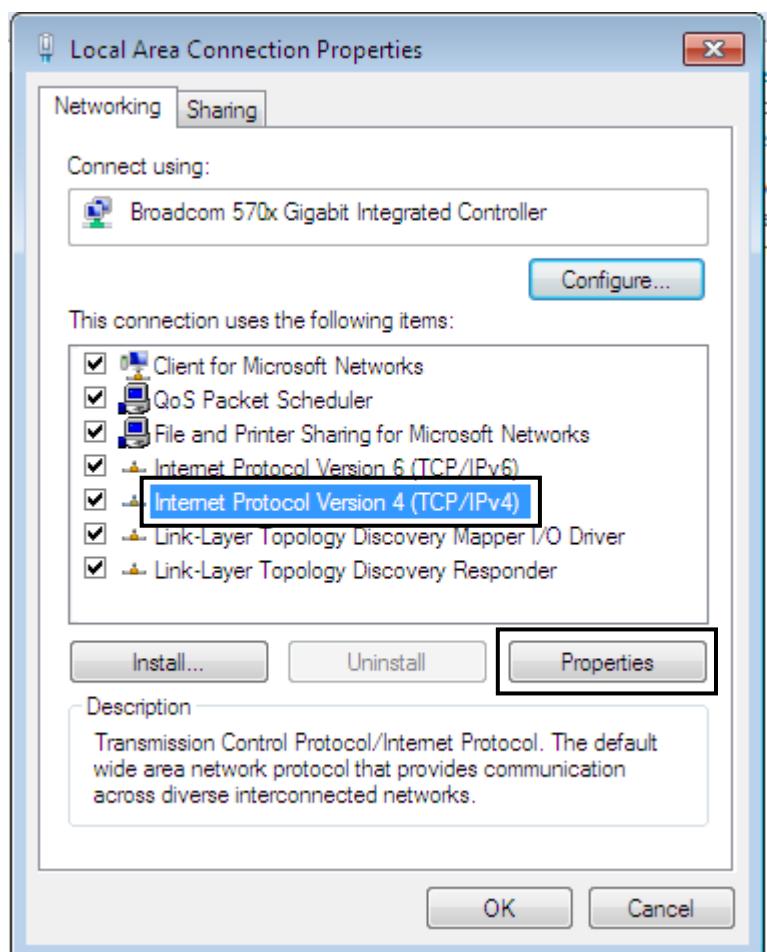
2. When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.



3. Select the Local Area Connection, and right click the icon to select Properties.

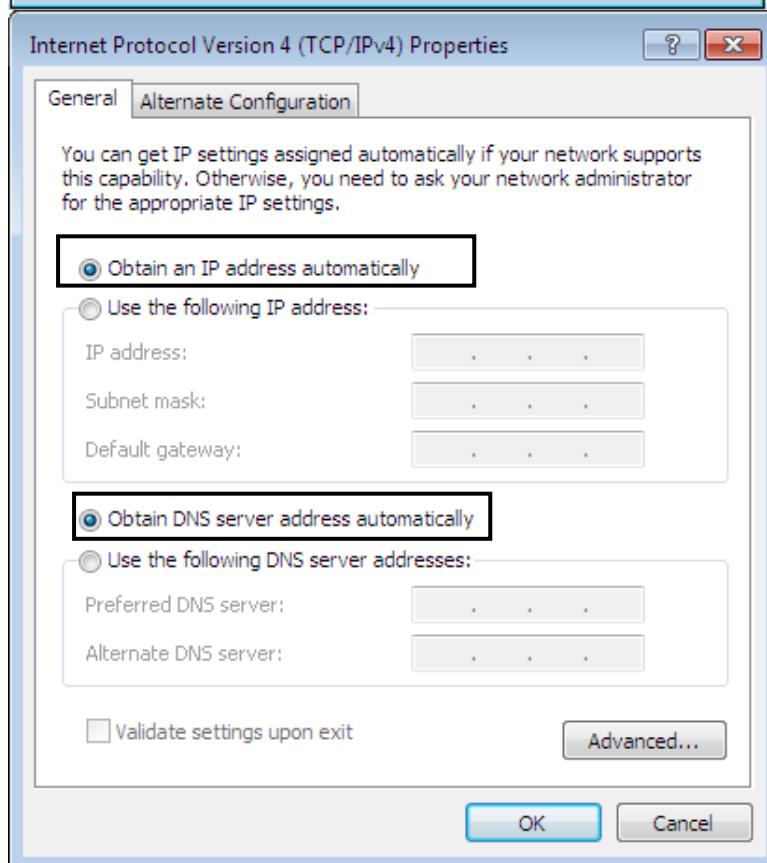


4. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



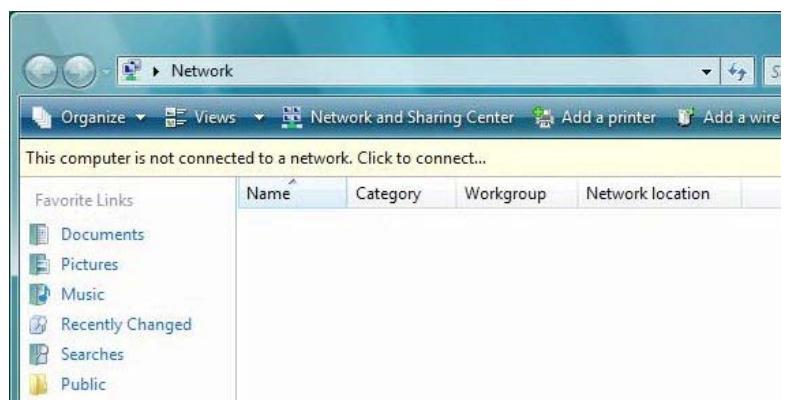
5. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.

6. Click OK again in the Local Area Connection Properties window to apply the new configuration.



Configuring PC in Windows Vista

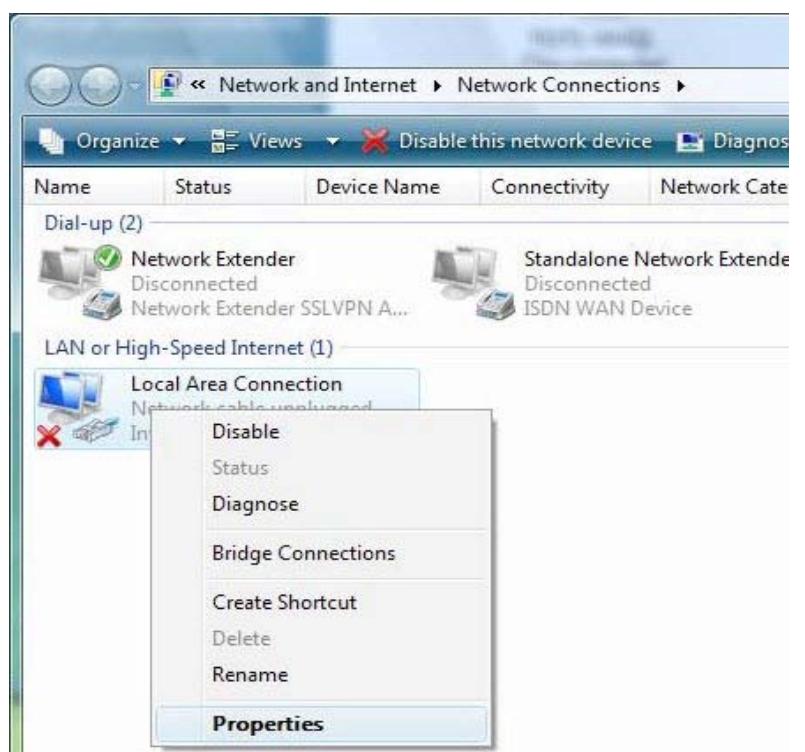
1. Go to Start. Click on Network.
2. Then click on Network and Sharing Center at the top bar.



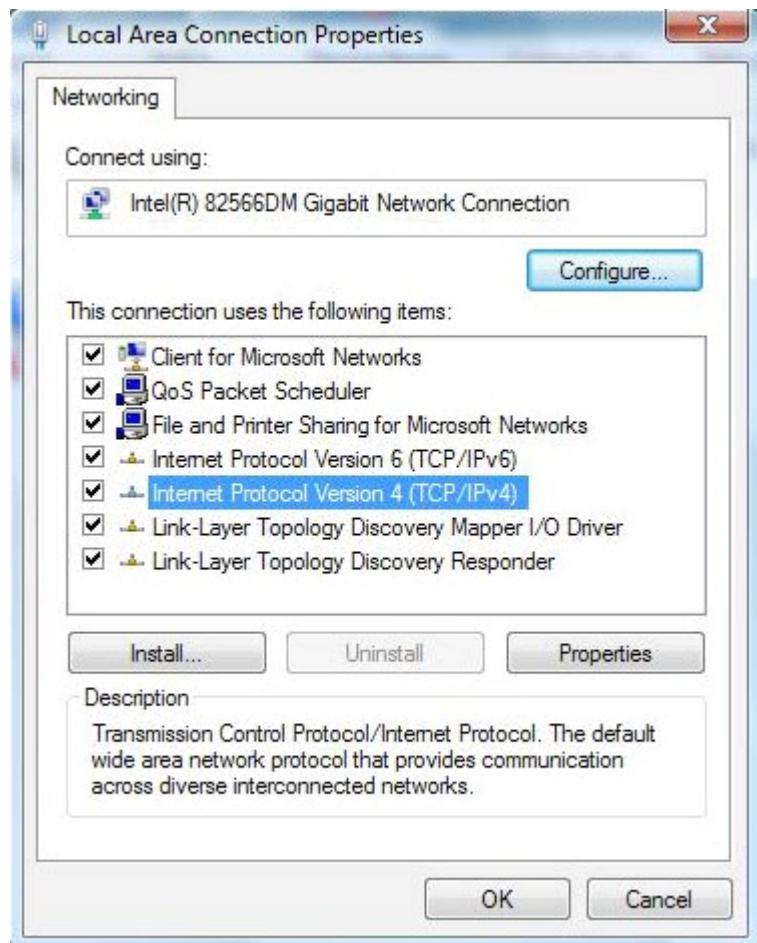
3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.



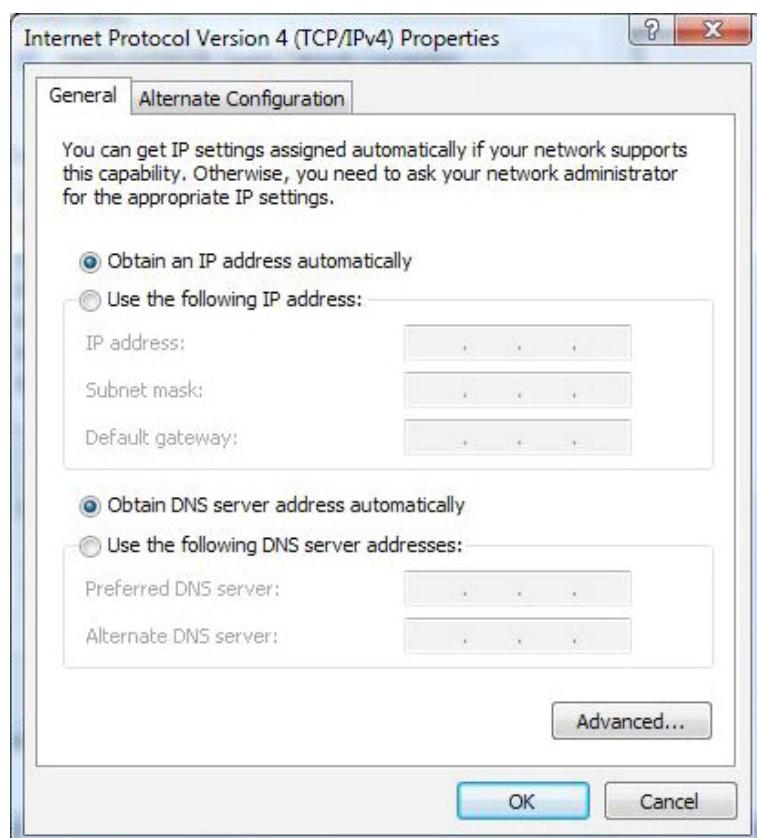
4. Select the Local Area Connection, and right click the icon to select Properties.



5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.
7. Click OK again in the Local Area Connection Properties window to apply the new configuration.

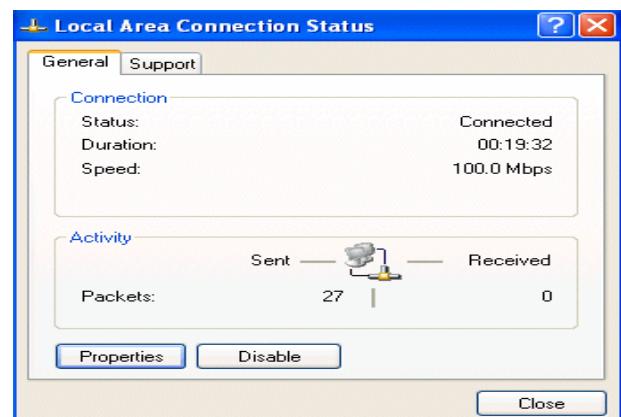


Configuring PC in Windows XP

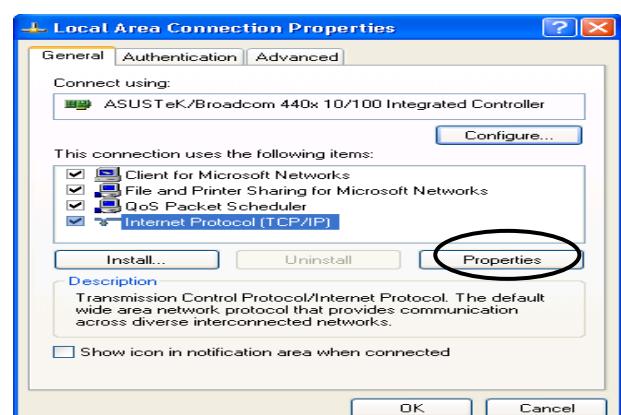
1. Go to Start > Control Panel (in Classic View). In the Control Panel, double-click on Network Connections
2. Double-click Local Area Connection.



3. In the Local Area Connection Status window, click Properties.

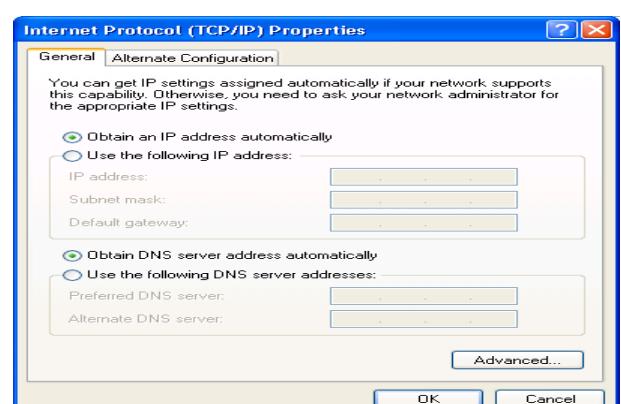


4. Select Internet Protocol (TCP/IP) and click Properties.



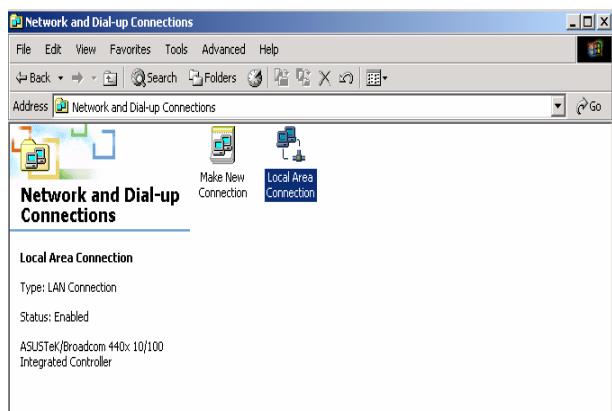
5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.

6. Click OK to finish the configuration.

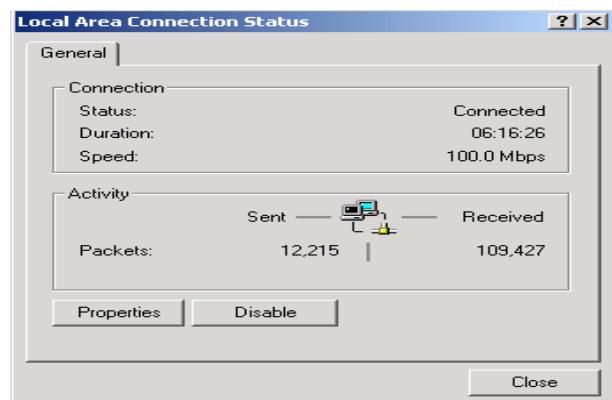


Configuring PC in Windows 2000

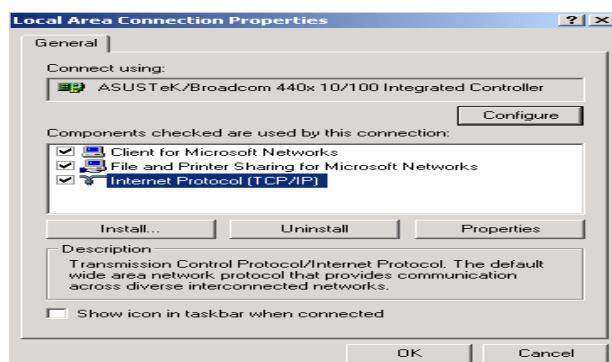
1. Go to Start > Settings > Control Panel.
In the Control Panel, double-click on Network and Dial-up Connections.
2. Double-click Local Area Connection.



3. In the Local Area Connection Status window click Properties.

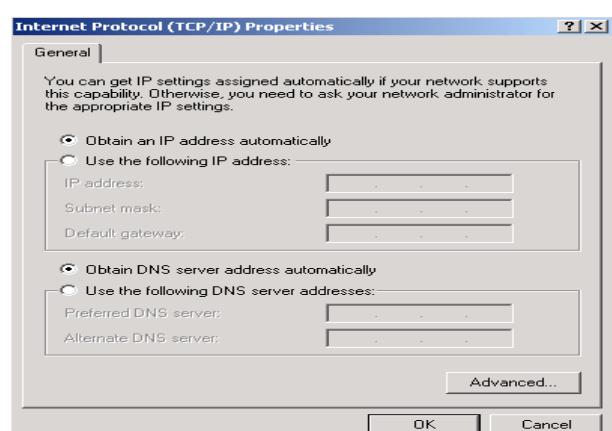


4. Select Internet Protocol (TCP/IP) and click Properties.



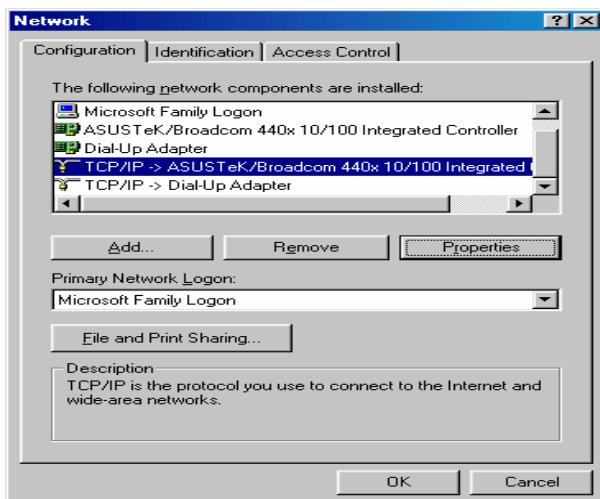
5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.

6. Click OK to finish the configuration.

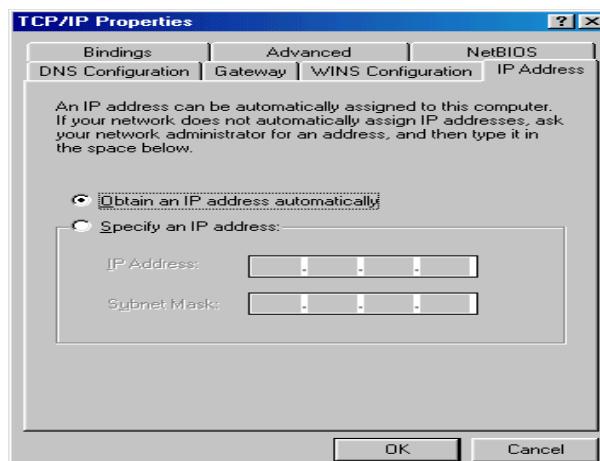


Configuring PC in Windows 95/98/Me

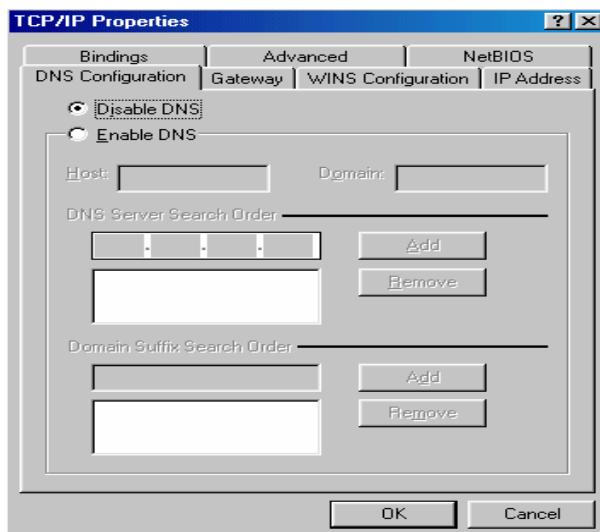
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Configuration tab.
2. Select TCP/IP > NE2000 Compatible, or the name of your Network Interface Card (NIC) in your PC.



3. Select the Obtain an IP address automatically radio button.

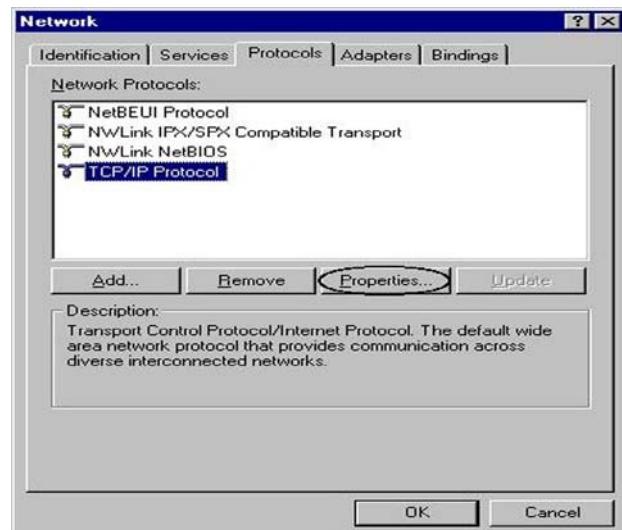


4. Then select the DNS Configuration tab.
5. Select the Disable DNS radio button and click OK to finish the configuration.

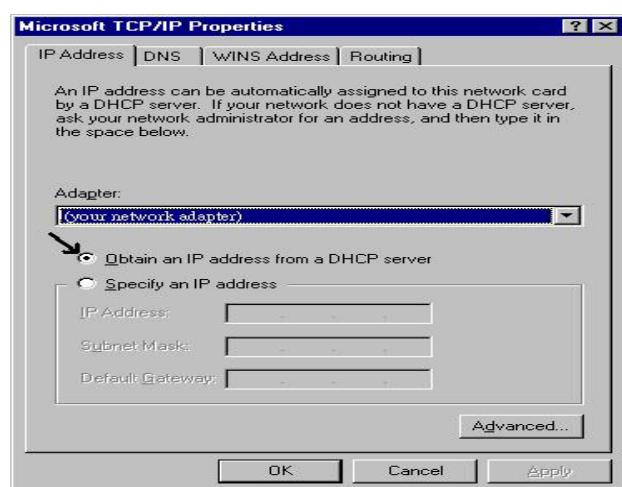


Configuring PC in Windows NT4.0

1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.
2. Select TCP/IP Protocol and click Properties.



3. Select the Obtain an IP address from a DHCP server radio button and click OK.



Factory Default Settings

Before configuring your router, you need to know the following default settings.

Web Interface (Username and Password)

Three user levels are provided by this router, thus **Administrator**, **Basic** and **Advanced** respectively. You can turn to [User Management](#) to change the corresponding passwords and understand more.

● Administrator

- ▶ Username: admin
- ▶ Password: admin

● Basic

- ▶ Username: user
- ▶ Password: user

● Advanced (for remote login)

- ▶ Username: support
- ▶ Password: support

The default username and password are “**admin**” and “**admin**” respectively.



Attention

If you have forgotten your username or password for the router, you can restore your device to its default setting by pressing the Reset button for more than **5** seconds.

Device LAN IP settings

- ▶ IP Address: 192.168.1.254
- ▶ Subnet Mask: 255.255.255.0

ISP setting in WAN site

- ▶ PPPoE

DHCP server

- ▶ DHCP server is enabled.
- ▶ Start IP Address: 192.168.1.100
- ▶ IP pool counts: 100

LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown in the table.

LAN Port		WAN Port
IP address	192.168.1.254	
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.

Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP (Obtain an IP Address Automatically, Static IP (Fixed IP Address) or PPPoE.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE(RFC2516)	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoA(RFC2364)	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
MPoA(RFC1483/ RFC2684)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA(RFC1577)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
Pure Bridge	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.

Chapter 4: Configuration

To easily configure this device for internet access, you must have IE 5.0 / Netscape 4.5 or above installed on your computer. There are basically 2 ways to configure your router before you are able to connect to the internet: **Easy Sign-On & Web Interface**. Configuration of each method will be discussed in detail in the following sections.

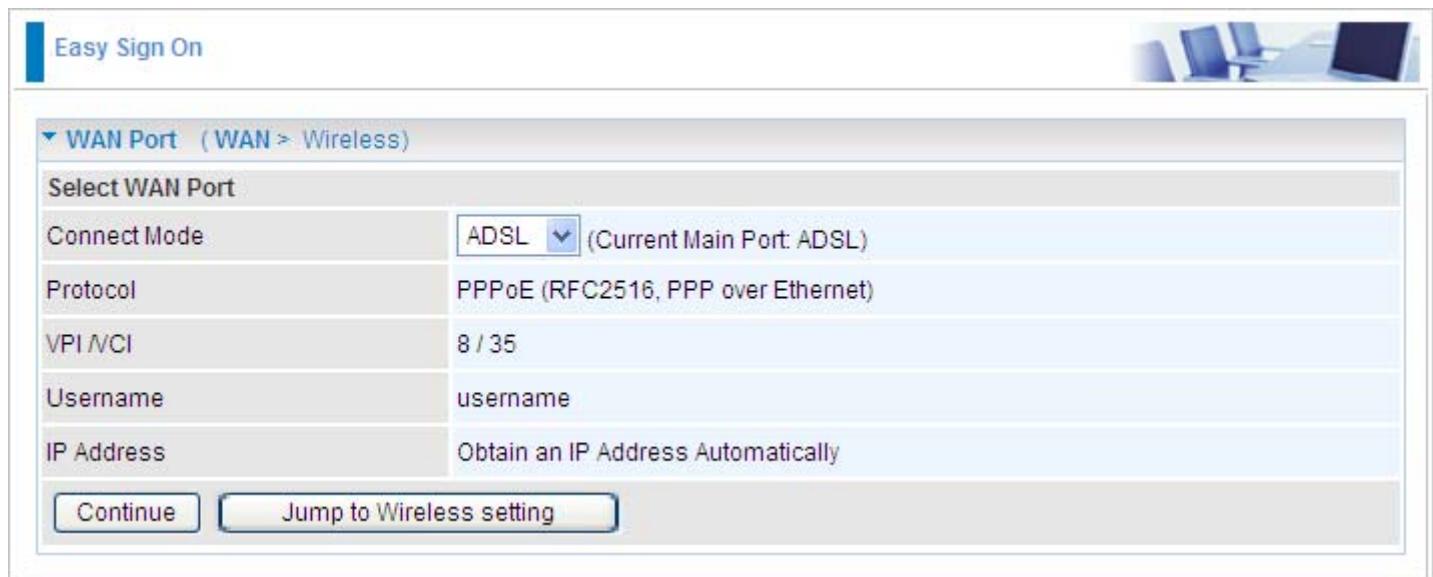
Easy Sign-On (EZSO)

This special feature makes it easier for you to configure your router so that you can connect to the internet in a matter of seconds without having to logon to the router GUI for any detail configuration. This configuration method is usually auto initiated if user is to connect to the internet via Billion's router for the first time.

After setting up the router with all the appropriate cables plugged-in, open up your IE browser, the EZSO WEB GUI will automatically pop up and request that you enter some basic information that you have obtained from your ISP. By following the instructions given carefully and through the information you provide, the router will be configured in no time and you will find yourself surfing the internet sooner than you realize.

Follow the Easy Sign-On configuration wizard to complete the basic network configuration.

1. Connect your router with all the appropriate cables. Then, load your IE / Netscape browser.
2. When the EZSO configuration wizard pops up, select the connect mode which you want to set up and then click continue. (There are three modes that you may select: "EWAN" "ADSL" and another is "3G".)



Easy Sign On

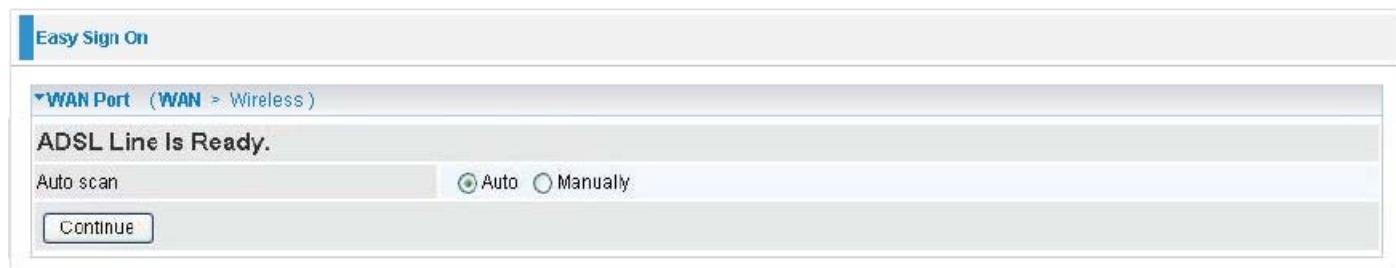
WAN Port (WAN > Wireless)

Select WAN Port

Connect Mode	ADSL (Current Main Port: ADSL)
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	8 / 35
Username	username
IP Address	Obtain an IP Address Automatically

Continue Jump to Wireless setting

3. Choose "Auto" or "Manually" to scan ADSL information.



Easy Sign On

WAN Port (WAN > Wireless)

ADSL Line Is Ready.

Auto scan Auto Manually

Continue

4. The window will then display the Protocol information obtained from the scan result before redirect you to the next configuration page.

Easy Sign On

▼WAN Port (WAN > Wireless)

Please wait while the ADSL is scanning.

[Abort to manually setting](#)

Easy Sign On

▼WAN Port (WAN > Wireless)

Auto scan result

Protocol	VPI/VCI 0/33 LLC PPPoE (RFC2516, PPP over Ethernet)
----------	---

5. Please enter all the information in the blanks provided and then click continue.

Quick Start

▼ WAN Port (WAN > Wireless)

Select protocol

Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	8 / 35
Username	username
Password	*****
Service Name	
Encapsulation method	LLC/SNAP-BRIDGING
Authentication Protocol	Auto
IP Address	0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically')
Obtain DNS Automatically	<input checked="" type="checkbox"/> Enable
Primary DNS / Secondary DNS	168.95.1.1 / 168.95.192.1
MTU	1492

[Continue](#)

6. The device will reboot and then load the new configuration.

Easy Sign On

▼ Restart

Since settings are changed, the router will reboot to make the changes take effect! Please wait for seconds.

total :	4%
---------	----

7. If all information provided is valid and the device successfully connects to WAN, a dialog box will appear to signify the completion of the WAN port setup. At this point you can either click Done to finish the EZSO configuration or you can click Next to wireless to proceed to the wireless configuration if you have.

Easy Sign On

WAN Port (WAN > Wireless)

Congratulations!
Your WAN port has been successfully configured.

[Next to Wireless](#) [Done](#)

8. Select Enable and enter the necessary information in the blanks provided for the Wireless LAN setting if you would like to use this feature and then click Continue.

Easy Sign On

Wireless (WAN > Wireless)

Set Wireless configuration.

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	wlan-ap
Channel ID	Channel 1 (2.412 GHz)
Security Mode	Disable

[Continue](#)

9. The system will save your new configuration and complete the setup.

Easy Sign On

Save configuration

Save configuration to FLASH. Please wait for 10 seconds

10. Congratulations! You've completed the setup and are now ready to surf the Internet.

Easy Sign On

Process finished

Success.
The Easy-Sign-On process is finished. Your device has been successfully configured.

11. You can test the connection by clicking on the URL link provided. If the setup is successful you will be redirected to website.

Easy Sign On

Process finished

Success.
The Easy-Sign-On process is finished. Your device has been successfully configured.

You can now:

1. Log onto the router management interface for more advanced settings on 192.168.1.254
2. Continue to tw.yahoo.com/index.html

Configuration via Web Interface

Open your web browser; enter the IP address of your router, which by default is 192.168.1.254, and click “Go”, a login window prompt will appear. The default username and password are “admin” and “admin” respectively.

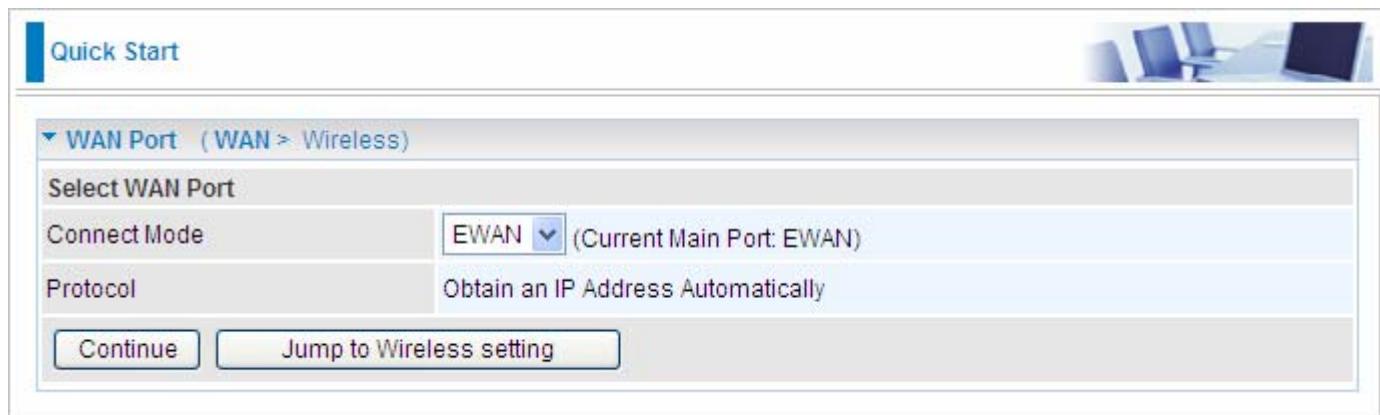


Congratulations! You are now successfully logon to the Firewall Router!

If the authentication succeeds, the homepage Status will appear on the screen.

Quick Start

Whether on the Basic or Advanced Configuration Mode, click Quick Start link to WAN Port setup pages.



Quick Start

▼ WAN Port (WAN > Wireless)

Select WAN Port

Connect Mode: EWAN (Current Main Port: EWAN)

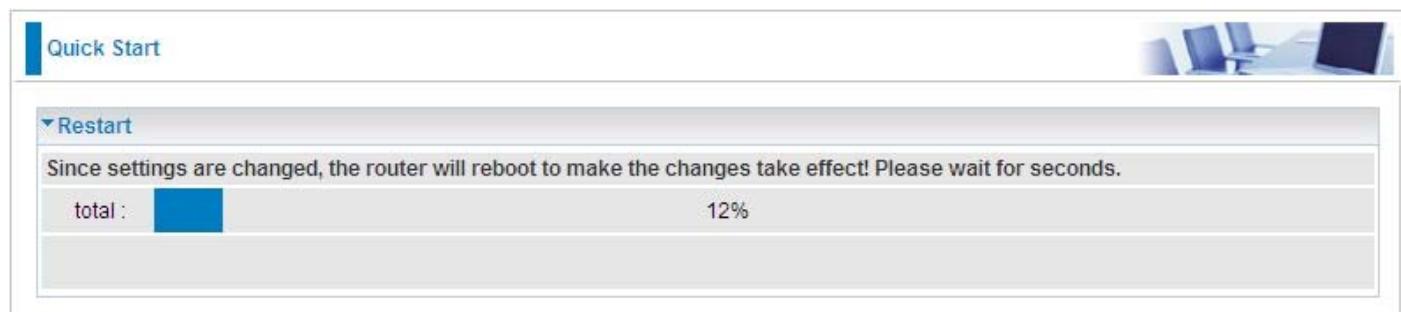
Protocol: Obtain an IP Address Automatically

Continue | Jump to Wireless setting

Step 1: Select WAN port connect mode from the connect mode drop down menu. There are three types of connect mode to choose from: EWAN, 3G or ADSL.

Step 2: After selecting the connect mode, press Continue to move on to the next configuring page. There are 5 types of phone service standards available for 3G connect mode while there are 5 types of connection protocols available under ADSL connect mode, 4 types of connection protocols available for EWAN connect mode. ***Each type of connection mode is described in the following sections of 3G Connect mode, ADSL Connect mode and EWAN Connect mode.***

Step 3: After finishing configuring the WAN port connection, click Continue to proceed. The system will upload and apply the new WAN port configuration to the device.



Quick Start

▼ Restart

Since settings are changed, the router will reboot to make the changes take effect! Please wait for seconds.

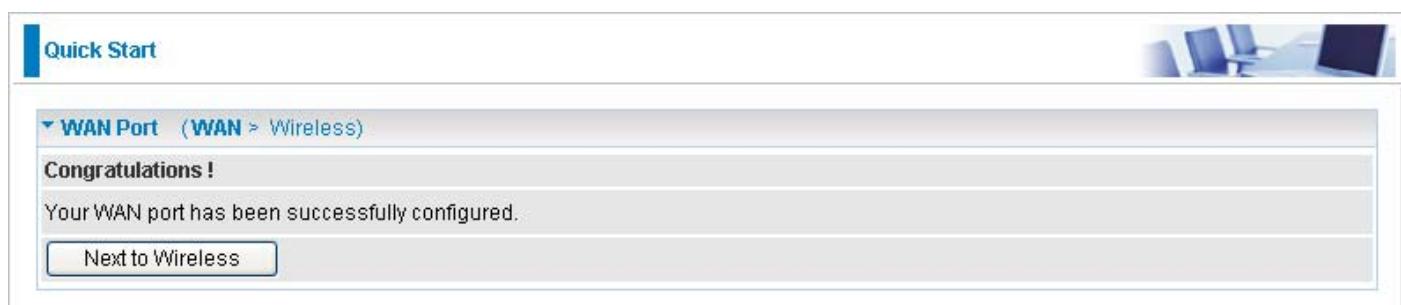
total: 12%



Quick Start

▼ WAN Port

Please wait while the device is configured.



Quick Start

▼ WAN Port (WAN > Wireless)

Congratulations!

Your WAN port has been successfully configured.

Next to Wireless | Jump to Wireless setting

Note: If the WAN line is not ready, a page will display as below and your new configuration can not be saved.

Quick Start

▼ WAN Port

Fail!!

WAN port setting is not successful, you can do this procedure again.

Step 4: After the configuration is successful, click Next to Wireless button and you may proceed to configure the Wireless setting. There are 4 types of security mode: WPA, WPA2, WPA/WPA2 Pre-Shared Key and WEP. Please refer to the [Wireless Setting Mode](#) section for detail description of each security mode.

Quick Start

▼ Wireless (WAN > Wireless)

Set Wireless configuration.

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	wlan-ap
Channel ID	Channel 1 (2.412 GHz)
Security Mode	Disable

Continue

Step 5: After finishing configuring the WLAN setting, press Continue to finish the Quick Start.

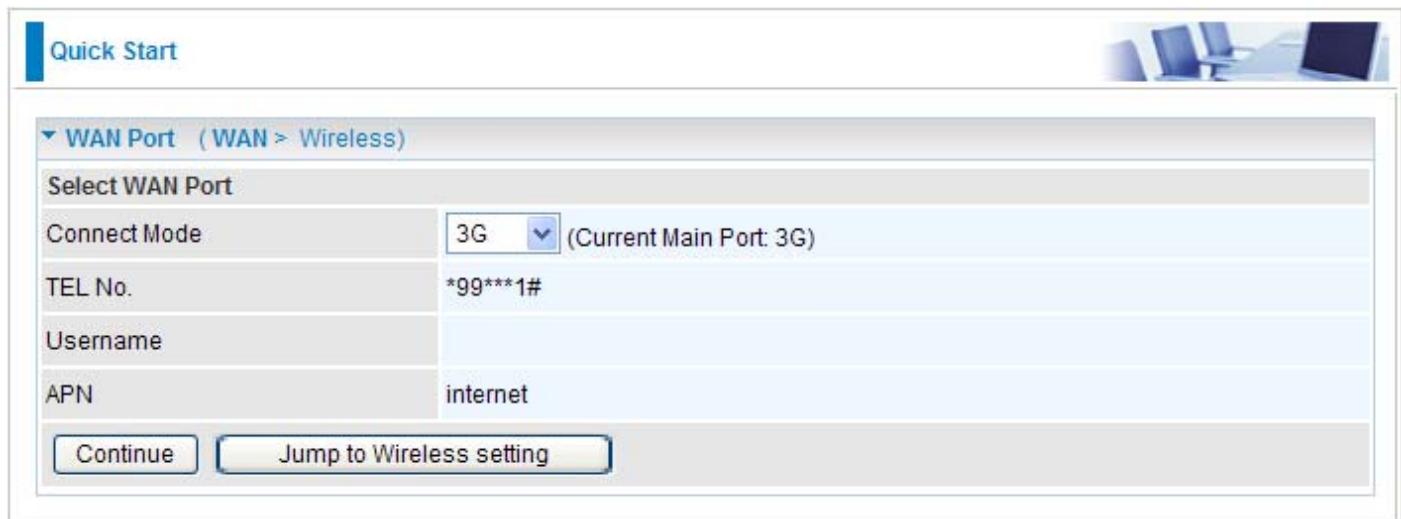
Quick Start

▼ Process finished

Success.

The Quick Start process is finished. Your device has been successfully configured.

3G Connect Mode



The screenshot shows the 'Quick Start' interface for 'WAN Port (WAN > Wireless)'. The 'Connect Mode' dropdown is set to '3G' (Current Main Port: 3G). The 'TEL No.' field contains the dial string '*99***1#'. The 'APN' field is set to 'internet'. Below the form are two buttons: 'Continue' and 'Jump to Wireless setting'.

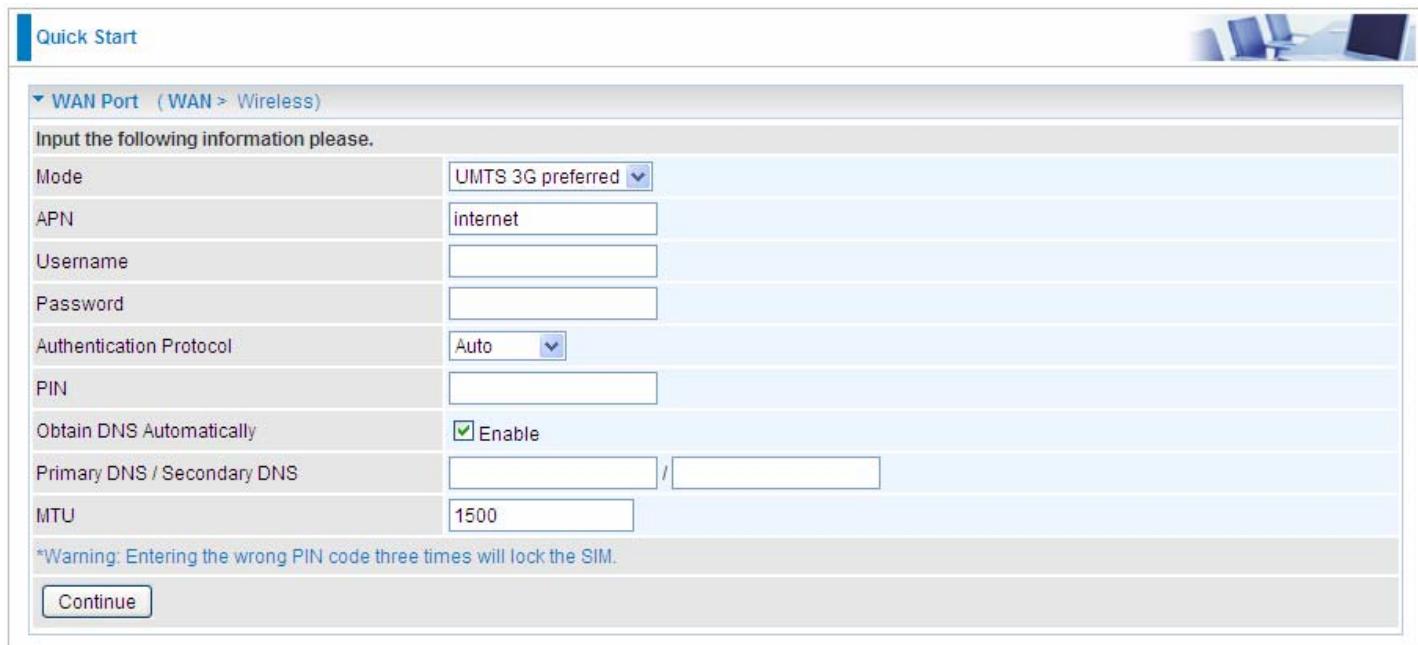
Connect Mode: Select “3G”.

TEL No.: The dial string to make a GPRS / 3G user internetworking call.

Username: The username provided by your service provider.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call.

Click **Continue** to go on to next step.



The screenshot shows the 'WAN Port (WAN > Wireless)' configuration page. It includes fields for Mode (UMTS 3G preferred), APN (internet), Username, Password, Authentication Protocol (Auto), PIN, Obtain DNS Automatically (checked), Primary DNS / Secondary DNS, and MTU (1500). A warning message at the bottom states: "Warning: Entering the wrong PIN code three times will lock the SIM." Below the form is a 'Continue' button.

Mode: There are 5 options of phone service standards: GSM 2G only, UMTS 3G only, GSM 2G preferred, UMTS 3G preferred, and Automatic. If you are uncertain what services are available to you, and then please select Automatic.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. Some 3G operators use the APN ‘internet’ for their portal. The default value is “internet”.

Username/Password: Enter the username and password provided by your ISP.

Authentication Protocol: Default is Auto. Please consult your ISP on whether to use PAP, CHAP or MSCHAP.

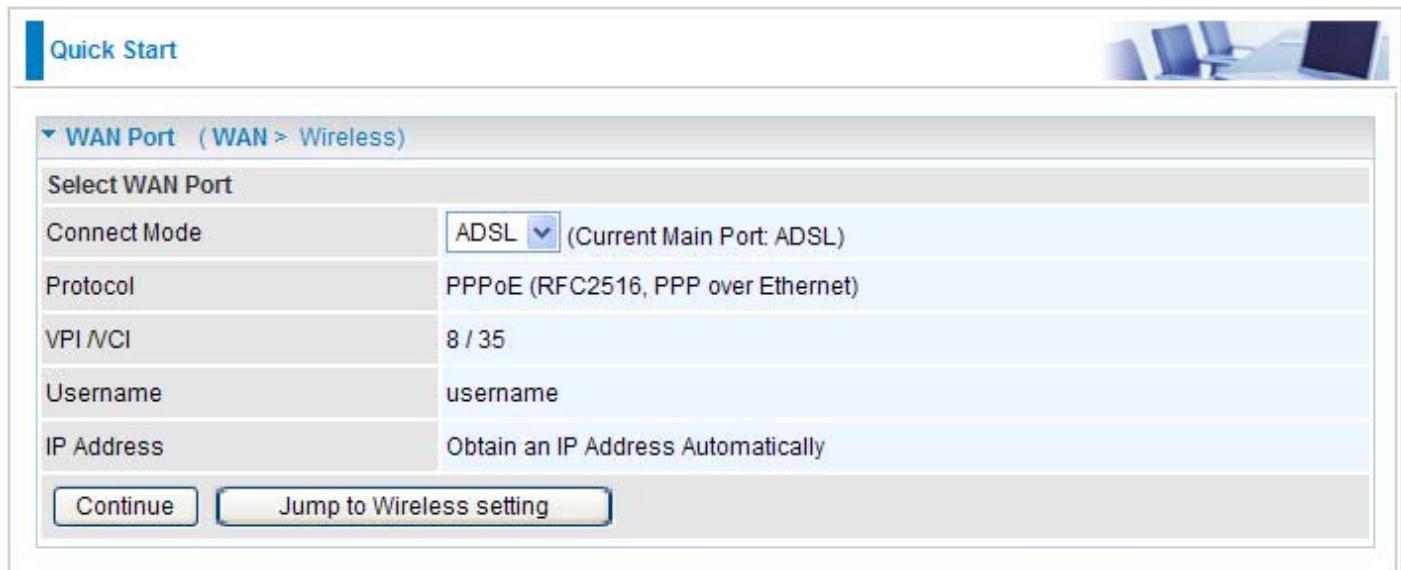
PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/service provider.

Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

MTU: Maximum Transmission Unit is the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

ADSL Connect Mode



Quick Start

WAN Port (WAN > Wireless)

Select WAN Port

Connect Mode	ADSL (Current Main Port: ADSL)
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI /VCI	8 / 35
Username	username
IP Address	Obtain an IP Address Automatically

Continue Jump to Wireless setting

Connect Mode: You can choose either “ADSL” “EWAN” or “3G” mode.

Protocol: The current ATM protocol in the device.

VPI/VCI: The current value of VPI/VCI in the device.

Username: To show current authentication username.

IP Address: To show current value of IP address in the device.

For ADSL connect mode there are 5 types of connection protocols: [PPPoE](#), [PPPoA](#), [IPoA](#), [MPoA](#) and [Pure Bridge](#).

PPPoE Connection



WAN Port (WAN > Wireless)

Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	8 / 35
Username	username
Password	*****
Service Name	
Encapsulation method	LLC/SNAP-BRIDGING
Authentication Protocol	Auto
IP Address	0.0.0.0 <small>('0.0.0.0' means 'Obtain an IP address automatically')</small>
Obtain DNS Automatically	<input checked="" type="checkbox"/> Enable
Primary DNS / Secondary DNS	168.95.1.1 / 168.95.192.1
MTU	1492

Continue

VPI/VCI: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

Authentication method: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

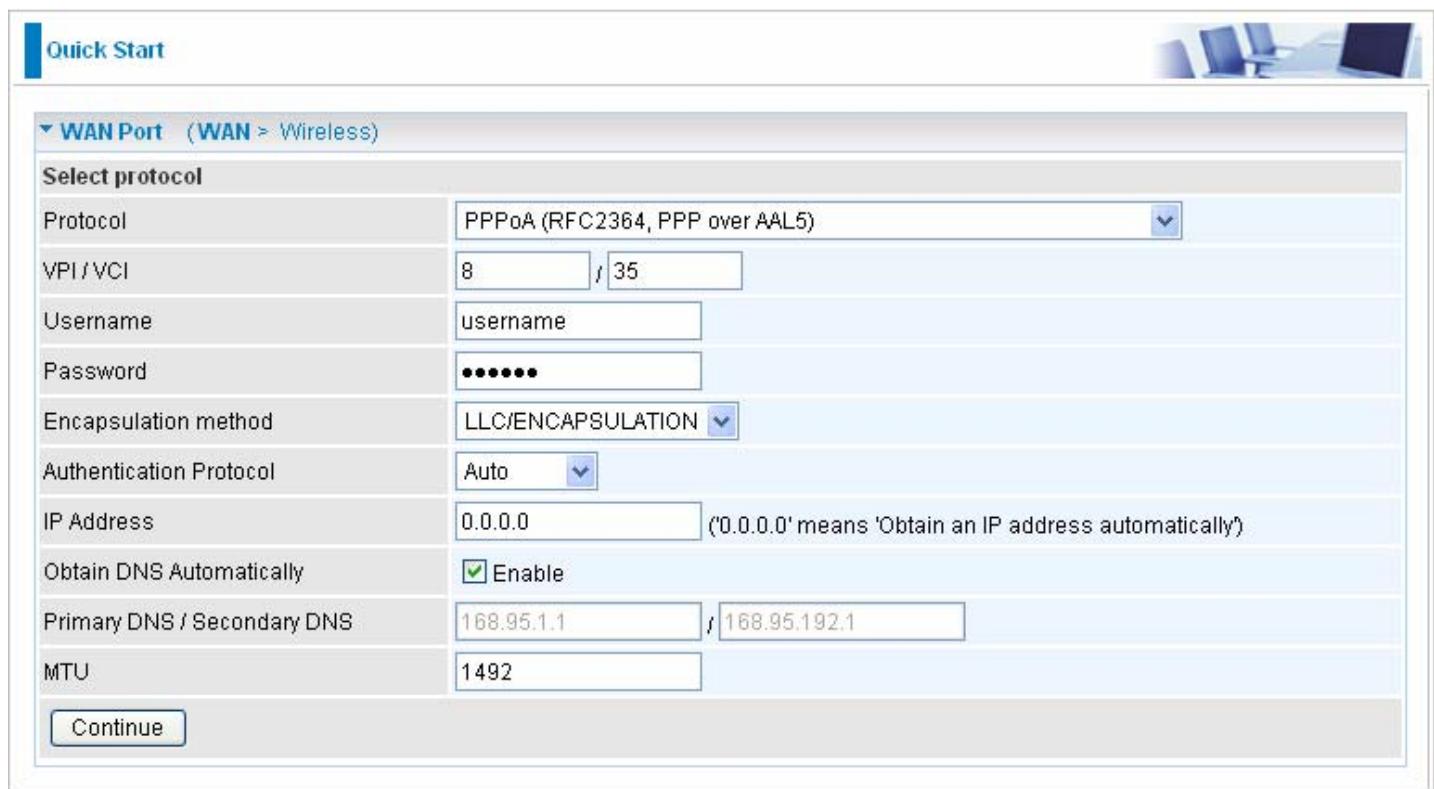
IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

MTU: MTU (Maximum Transmission Unit.) is the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

PPPoA Connection



The screenshot shows a configuration interface for a PPPoA connection. The 'Protocol' is set to 'PPPoA (RFC2364, PPP over AAL5)'. The 'VPI / VCI' is set to '8 / 35'. The 'Username' is 'username' and the 'Password' is masked. The 'Encapsulation method' is 'LLC/ENCAPSULATION'. The 'Authentication Protocol' is 'Auto'. The 'IP Address' is '0.0.0.0' with a note '(0.0.0.0' means 'Obtain an IP address automatically)'). The 'Obtain DNS Automatically' checkbox is checked. The 'Primary DNS / Secondary DNS' fields are '168.95.1.1' and '168.95.192.1'. The 'MTU' is '1492'. A 'Continue' button is at the bottom.

VPI/VCI: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

Authentication method: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

MTU: MTU (Maximum Transmission Unit) is the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

MPoA Connection

Quick Start

WAN Port (WAN > Wireless)

Select protocol

Protocol: MPoA (RFC1483/RFC2684, Multiprotocol Encapsulation over AAL5)

VPI / VCI: 8 / 35

Encapsulation method: LLC/SNAP-BRIDGING

IP Address: 0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically')

Netmask: 255.255.255.0

Gateway:

Obtain DNS Automatically: Enable

Primary DNS / Secondary DNS: 168.95.1.1 / 168.95.192.1

Continue

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: IPOA WAN IP address can only set fixed IP address.

Netmask: User can change it to others such as 255.255.255.128. Type the Netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

IPoA Connection

Quick Start

WAN Port (WAN > Wireless)

Select protocol

Protocol: IPoA (RFC1577, Classic IP and ARP over ATM)

VPI / VCI: 8 / 35

Encapsulation method: LLC/ROUTING

IP Address: (empty)

Netmask: 255.255.255.0

Gateway: (empty)

Obtain DNS Automatically: Enable

Primary DNS / Secondary DNS: 168.95.1.1 / 168.95.192.1

Continue

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: Your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both Netmask and gateway may be left blank.

Netmask: User can change it to others such as 255.255.255.128. Type the Netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

Pure Bridge Connection

Quick Start

WAN Port (WAN > Wireless)

Select protocol

Protocol	Pure Bridge
VPI / VCI	8 / 35
Encapsulation method	LLC/SNAP-BRIDGING

Continue

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

EWAN Connect Mode

PPPoE Connection

Quick Start

WAN Port (WAN > Wireless)

Select protocol

Protocol	PPPoE
Username	username
Password	*****
Service Name	
Authentication Protocol	Auto
IP Address	0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically')
Obtain DNS Automatically	<input checked="" type="checkbox"/> Enable
Primary DNS / Secondary DNS	168.95.1.1 / 168.95.192.1
MTU	1492

Continue

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive). This is in the format of "username@ispname" instead of simply "username".

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

Authentication method: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

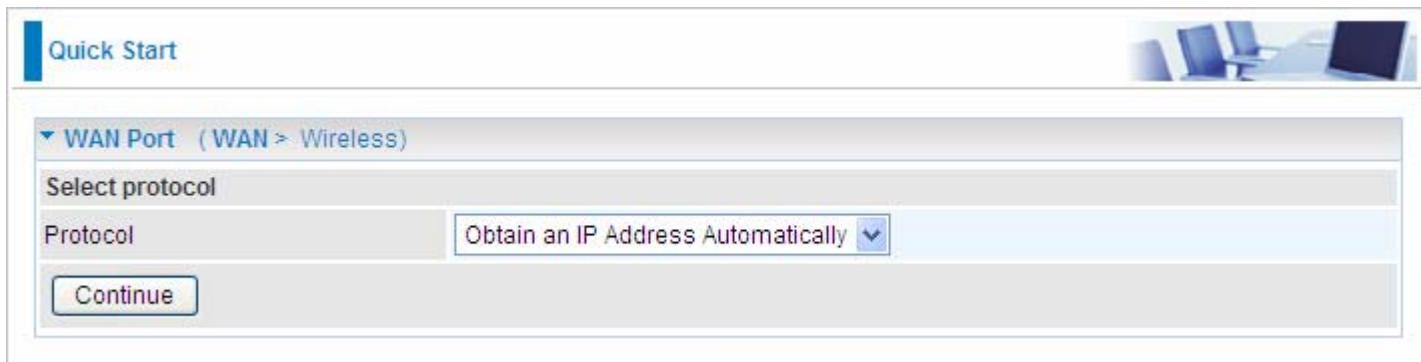
Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

MTU: MTU (Maximum Transmission Unit.) is the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Obtain an IP Address Automatically

Select this protocol enables the device to automatically retrieve IP address.



Quick Start

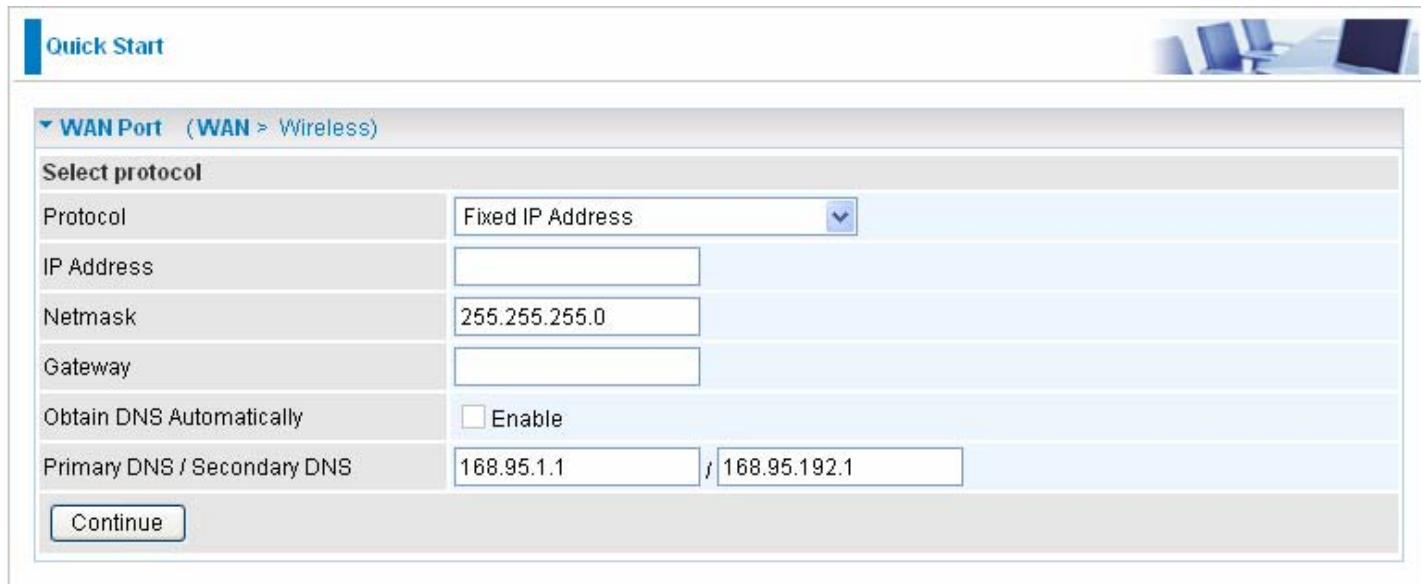
WAN Port (WAN > Wireless)

Select protocol

Protocol: Obtain an IP Address Automatically

Continue

Fixed IP Address Connection



Quick Start

WAN Port (WAN > Wireless)

Select protocol

Protocol: Fixed IP Address

IP Address: (empty)

Netmask: 255.255.255.0

Gateway: (empty)

Obtain DNS Automatically: Enable

Primary DNS / Secondary DNS: 168.95.1.1 / 168.95.192.1

Continue

IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Netmask: The default is 0.0.0.0. User can change it to other such as 255.255.255.0. Type the subnet mask assigned to you by your ISP (if given).

Gateway: You must specify a gateway IP address (supplied by your ISP).

Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

Pure Bridge

Quick Start

WAN Port (WAN > Wireless)

Select protocol

Protocol: Pure Bridge

Continue

Wireless Setting Mode

Quick Start

Wireless (WAN > Wireless)

Set Wireless configuration.

WLAN Service: Enable Disable

ESSID: wlan-ap

Channel ID: Channel 1 (2.412 GHz)

Security Mode: Disable

Continue

There are 4 types of wireless security modes: [WPA](#), [WPA2](#), [WPA/WPA2 Pre-Shared Key](#) and [WEP](#).

WPA or WPA2

Here take WPA for example.



The screenshot shows the 'Wireless' configuration page with the following settings:

Set Wireless configuration.	
WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	wlan-ap
Channel ID	Channel 1 (2.412 GHz)
Security Mode	WPA
RADIUS / 802.1x	<input type="checkbox"/> Enable
WPA Shared Key	[Empty text field]

Continue

WLAN Service: Default setting is Enable. If you want to use wireless, you can select Enable.

ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

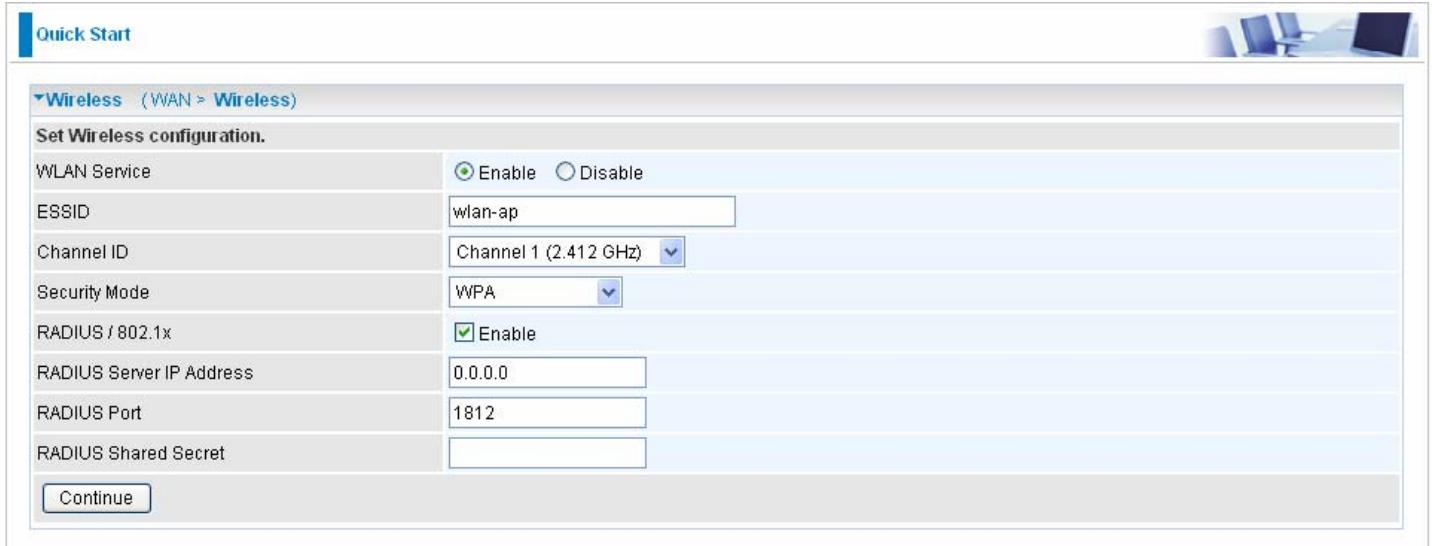
Channel ID: Select the channel ID that you would like to use.

Security Mode: You can disable or enable with WPA or WEP to protect wireless network. The default mode of wireless security is Disable.

RADIUS/802.1x: Select Whether to enable or disable the RADIUS Service.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

If you want to enable the RADIUS service, check Enable and then do the following settings.



The screenshot shows the 'Wireless' configuration page with the following settings, including RADIUS configuration:

Set Wireless configuration.	
WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	wlan-ap
Channel ID	Channel 1 (2.412 GHz)
Security Mode	WPA
RADIUS / 802.1x	<input checked="" type="checkbox"/> Enable
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Shared Secret	[Empty text field]

Continue

RADIUS Server IP Address: Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here. Default value is 1812.

RADIUS Shared Secret: Enter the password of RADIUS authentication server.

WPA/WPA2 Pre-Shared Key

WPA and WPA2 pre-shared keys are an authentication mechanism in which users provides some form of credentials to verify that they should be allowed access to a network. This requires a single password entered into each WLAN node (Access Points, Wireless Routers, client adapters, bridges). As long as the passwords match, a client will be granted access to a WLAN.



Quick Start

Wireless (WAN > Wireless)

Set Wireless configuration.

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	wlan-ap
Channel ID	Channel 1 (2.412 GHz)
Security Mode	WPA/WPA2-PSK
WPA Shared Key	[Input Field]

Continue

WLAN Service: Default setting is Enable. If you want to use wireless, you can select Enable.

ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

Channel ID: Select the channel ID that you would like to use.

Security Mode: You can disable or enable with WPA or WEP to protect wireless network. The default mode of wireless security is Disable.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

WEP

Quick Start

Wireless (WAN > Wireless)

Set Wireless configuration.

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	wlan-ap
Channel ID	Channel 1 (2.412 GHz)
Security Mode	WEP
RADIUS / 802.1x	<input type="checkbox"/> Enable
Default Used WEP Key	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4
Key	[Key Input Field]

WEP 64 - Hex: 10 Hex codes, (0~9, a~f, A~F). EX: 11aa22cc33.
WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.
WEP 128 - Hex: 26 Hex codes, (0~9, a~f, A~F). EX: 11aa22cc33dd44ee55efffe35f.
WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?l!dbd3ert.

[Continue](#)

WLAN Service: Default setting is set to Enable. If you want to use wireless, you can select Enable.

ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

Channel ID: Select the channel ID that you would like to use.

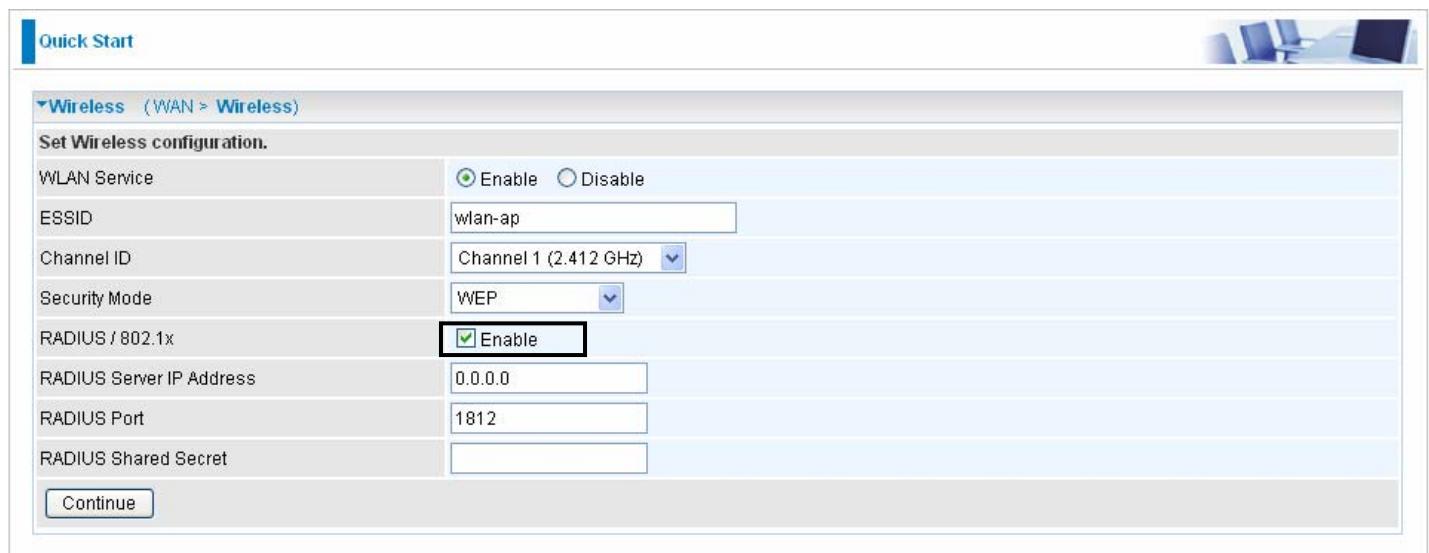
Security Mode: You can disable or enable with WPA or WEP to protect wireless network. The default mode of wireless security is Disable.

RADIUS/802.1x: Choose this box enable RADIUS/802.1x authentication protocol for boosting up WLAN Security.

Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Key (1~4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format can either be HEX style or ASCII format, 10 and 26 HEX codes or 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively.

If you want to enable the RADIUS service, check Enable and then do the following settings.



The screenshot shows a configuration interface for a wireless service. The 'WLAN Service' is set to 'Enable'. The 'ESSID' is 'wlan-ap'. The 'Channel ID' is 'Channel 1 (2.412 GHz)'. The 'Security Mode' is 'WEP'. The 'RADIUS / 802.1x' section has a checked 'Enable' checkbox, which is highlighted with a black box. The 'RADIUS Server IP Address' is '0.0.0.0', the 'RADIUS Port' is '1812', and the 'RADIUS Shared Secret' field is empty. A 'Continue' button is at the bottom.

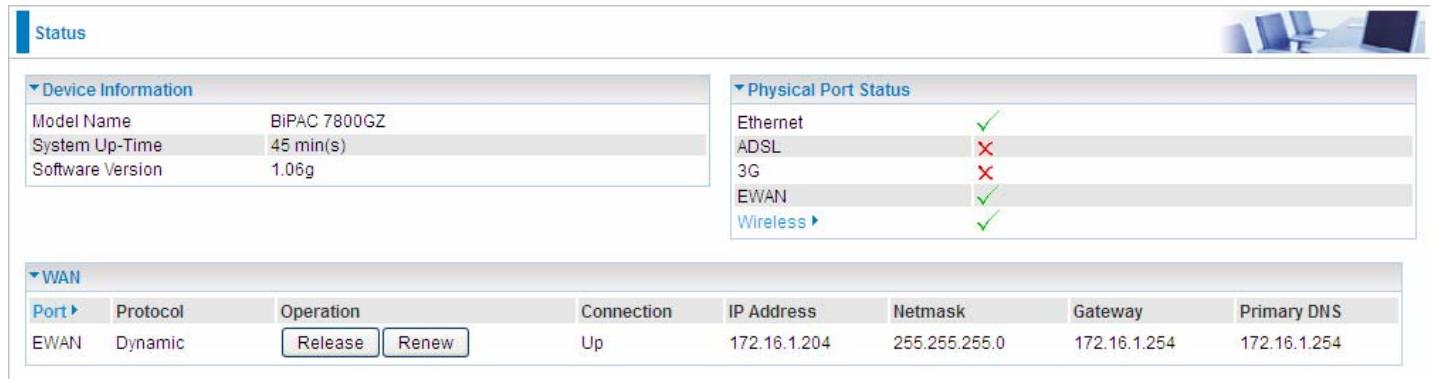
RADIUS Server IP Address: Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here. Default value is 1812.

RADIUS Shared Secret: Enter the password of RADIUS authentication server.

Basic Configuration Mode

Status



The screenshot shows the 'Status' page of a network device. It includes sections for 'Device Information', 'Physical Port Status', and 'WAN' settings.

Device Information:

Model Name	BiPAC 7800GZ
System Up-Time	45 min(s)
Software Version	1.06g

Physical Port Status:

Ethernet	✓
ADSL	✗
3G	✗
EWAN	✓
Wireless	✓

WAN:

Port	Protocol	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
EWAN	Dynamic	<button>Release</button> <button>Renew</button>	Up	172.16.1.204	255.255.255.0	172.16.1.254	172.16.1.254

Device Information

Model Name: Provide a name for the router for identification purposes.

System Up-Time: Record system up-time.

Hardware Version: Hardware version.

Software Version: Firmware version.

Port Status

Port Status: User can look up to see if they are connected to Ethernet, ADSL, 3G, EWAN and Wireless.

WAN

Port: Name of the WAN connection, ADSL, EWAN or 3G.

Protocol: the current used protocol for the connection.

Operation: Current status in WAN interface.

Connection: Current connection status.

IP Address: WAN port IP address.

Netmask: WAN port IP subnet mask.

Gateway: IP address of the default gateway.

Primary DNS: IP address of the primary DNS server.

WAN – Main Port (ADSL)

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

PPPoE Connection (ADSL)

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.

WAN Port	
Parameters	
Main Port	ADSL (Current Main Port: ADSL)
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	8 / 35
Username	username
Password	*****
Service Name	
Encap. method	LLC/SNAP-BRIDGING
Auth. Protocol	Auto
IP Address	0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically')
Obtain DNS Automatically	<input checked="" type="checkbox"/> Enable
Primary DNS / Secondary DNS	168.95.1.1 / 168.95.192.1
MTU	1492
<input type="button" value="Apply"/>	

VPI/VCI: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

IP Address: Enter your WAN IP address. Leave the IP address empty or enter 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Click Apply to confirm the settings.

PPPoA Connection (ADSL)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functionality in a manner similar to dial-up services using PPP.

Parameters	
Main Port	ADSL (Current Main Port: ADSL)
Protocol	PPPoA (RFC2364, PPP over AAL5)
VPI / VCI	8 / 35
Username	username
Password	*****
Encap. method	LLC/ENCAPSULATION
Auth. Protocol	Auto
IP Address	0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically')
Obtain DNS Automatically	<input checked="" type="checkbox"/> Enable
Primary DNS / Secondary DNS	168.95.1.1 / 168.95.192.1
MTU	1492

VPI/VCI: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

IP Address: Enter your WAN IP address. Leave the IP address empty or enter 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

MTU: MTU (Maximum Transmission Unit) is the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Click Apply to confirm the settings.

MPoA Connection (ADSL)

The screenshot shows a configuration interface with a 'Configuration' header and a 'WAN Port' section. The 'Parameters' group contains the following fields:

Main Port	ADSL (Current Main Port: ADSL)
Protocol	MPoA (RFC1483/RFC2684, Multiprotocol Encapsulation over AAL5)
VPI / VCI	8 / 35
Encap. method	LLC/SNAP-BRIDGING
IP Address	0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically')
Netmask	255.255.255.0
Gateway	[Blank]
Obtain DNS Automatically	<input checked="" type="checkbox"/> Enable
Primary DNS / Secondary DNS	168.95.1.1 / 168.95.192.1

At the bottom left is an 'Apply' button.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: Enter your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both Netmask and gateway may be left blank.

Netmask: User can change it to others such as 255.255.255.128. Type the Netmask assigned to you by your ISP (if given).

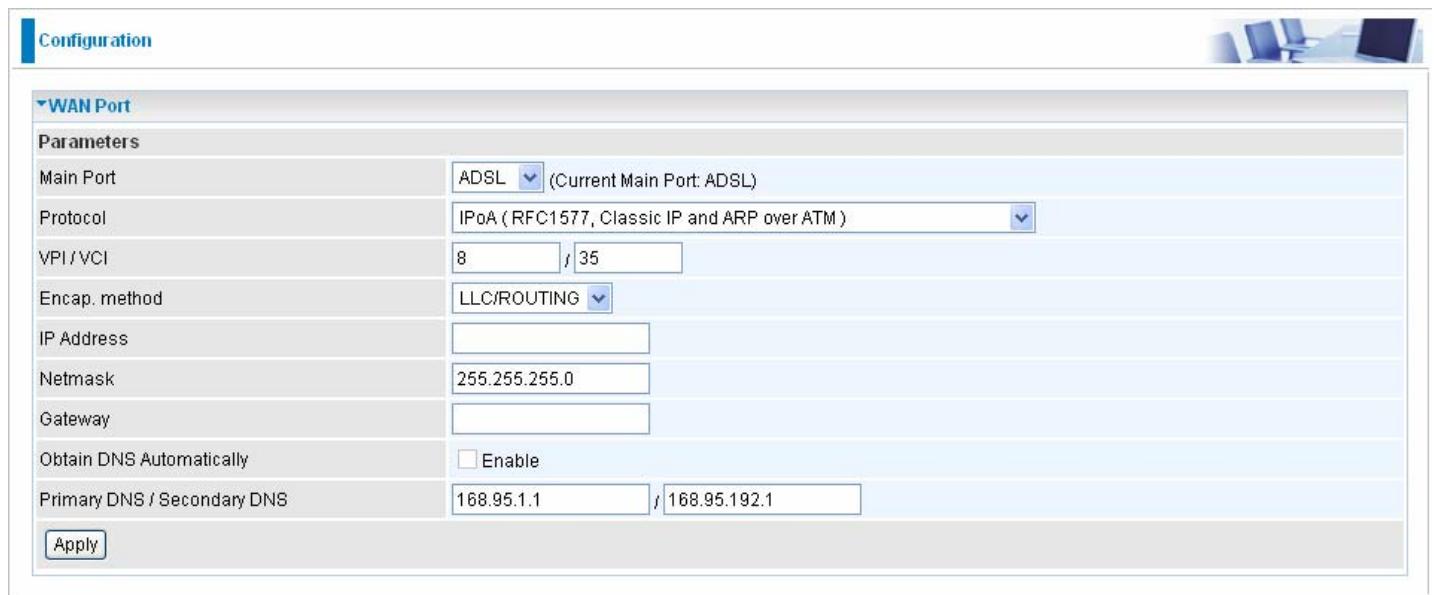
Gateway: Enter the IP address of the default gateway.

Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

Click Apply to confirm the settings.

IPoA Connections (ADSL)



The screenshot shows a configuration interface for a WAN port. The main section is titled 'WAN Port' and contains the following parameters:

Main Port	ADSL (Current Main Port: ADSL)
Protocol	IPoA (RFC1577, Classic IP and ARP over ATM)
VPI / VCI	8 / 35
Encap. method	LLC/ROUTING
IP Address	[Empty]
Netmask	255.255.255.0
Gateway	[Empty]
Obtain DNS Automatically	<input type="checkbox"/> Enable
Primary DNS / Secondary DNS	168.95.1.1 / 168.95.192.1

At the bottom left is a 'Apply' button.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: Enter your fixed IP address.

Netmask: User can change it to others such as 255.255.255.128. Type the Netmask assigned to you by your ISP (if given).

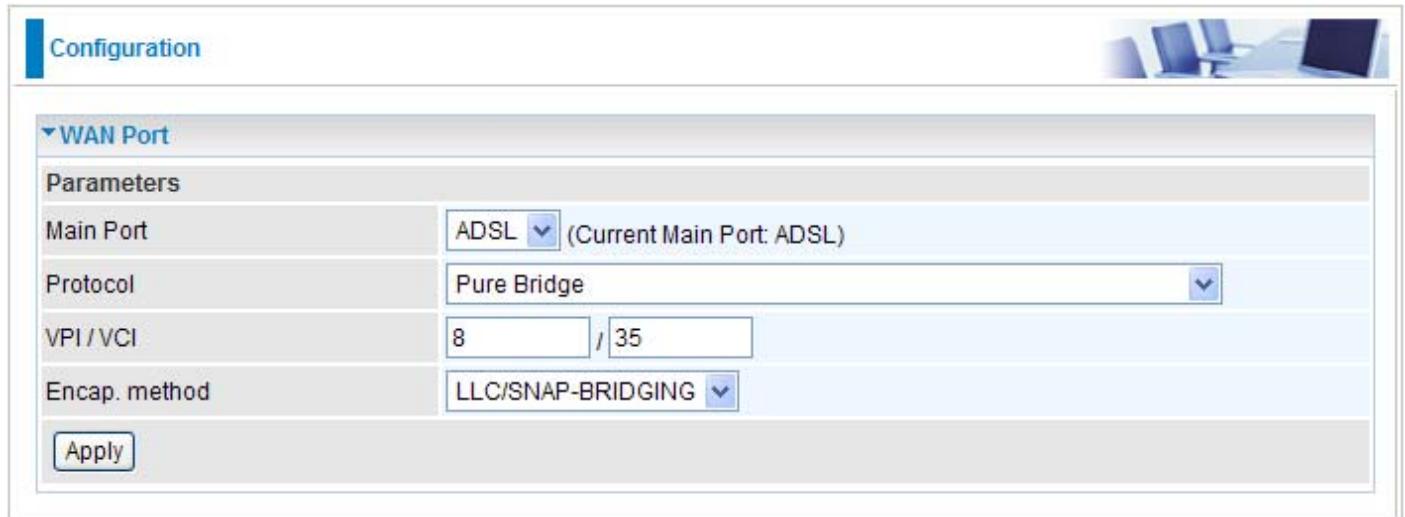
Gateway: Enter the IP address of the default gateway.

Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

Click Apply to confirm the settings.

Pure Bridge Connections (ADSL)



The screenshot shows a 'Configuration' interface with a 'WAN Port' section. The 'Protocol' is set to 'Pure Bridge'. Other settings include 'Main Port' (ADSL), 'VPI / VCI' (8 / 35), and 'Encap. method' (LLC/SNAP-BRIDGING). An 'Apply' button is visible.

Parameters	
Main Port	ADSL (Current Main Port: ADSL)
Protocol	Pure Bridge
VPI / VCI	8 / 35
Encap. method	LLC/SNAP-BRIDGING

Apply

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Click Apply to confirm the settings.

WAN – Main Port (EWAN)

Besides using ADSL to get connected to the Internet, Ethernet port 4 of BiPAC 7800GZ(L) can be used as an alternative to connect to Cable Modems, VDSL and fiber optic lines. This alternative not only provides faster connection to the Internet, it also provides users with more flexibility to get online.

PPPoE (EWAN)

The screenshot shows the 'WAN Port' configuration page. The 'Main Port' is set to 'EWAN' (Current Main Port: ADSL). The 'Protocol' is set to 'PPPoE'. The 'Username' field contains 'username'. The 'Password' field contains '*****'. The 'Service Name' field is empty. The 'Auth. Protocol' is set to 'Auto'. The 'IP Address' field is set to '0.0.0.0' with a note: '(0.0.0.0' means 'Obtain an IP address automatically')'. The 'Obtain DNS Automatically' checkbox is checked. The 'Primary DNS / Secondary DNS' field contains '168.95.1.1 / 168.95.192.1'. The 'MTU' is set to '1492'. At the bottom is an 'Apply' button.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

IP Address: Enter your fixed IP address.

Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

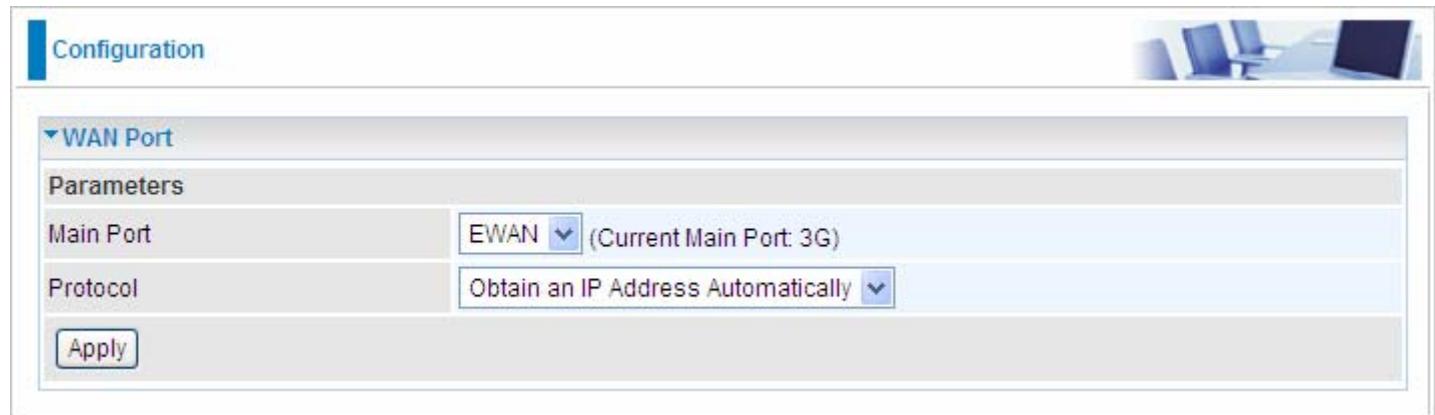
Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

MTU: MTU (Maximum Transmission Unit) is the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Click Apply to confirm the settings.

Obtain IP Address Automatically (EWAN)

Select this protocol enables the device to automatically retrieve IP address.

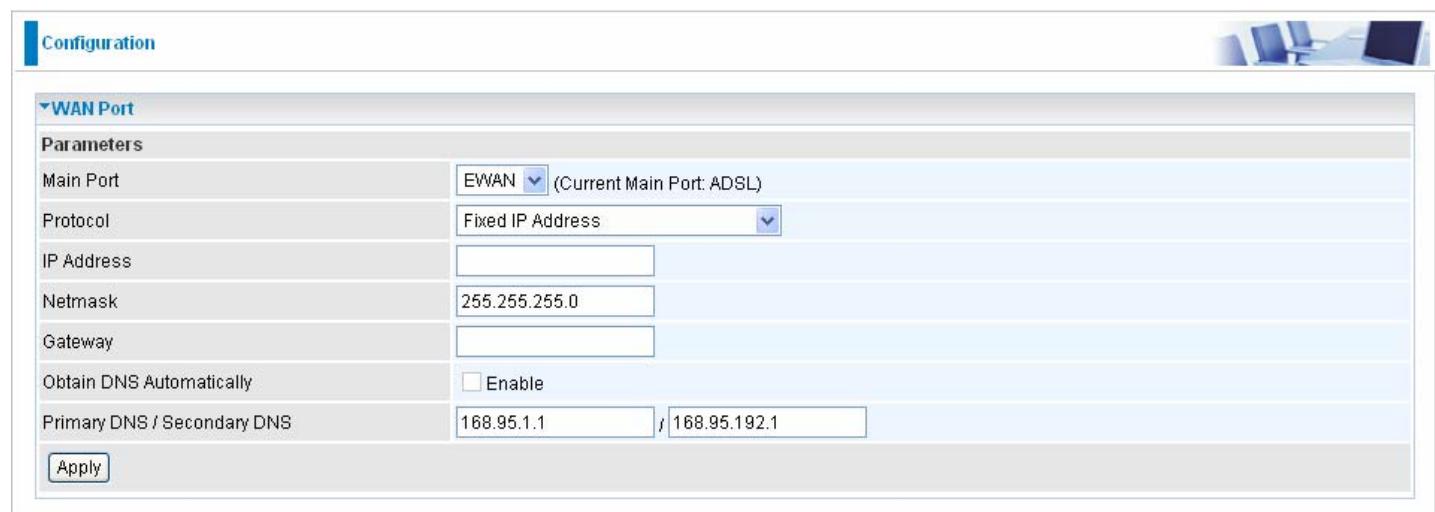


The screenshot shows the 'Configuration' interface with the 'WAN Port' section selected. Under 'Parameters', the 'Main Port' is set to 'EWAN' and the 'Protocol' is set to 'Obtain an IP Address Automatically'. An 'Apply' button is visible at the bottom.

Main Port: Choose **EWAN** as the main port.

Click **Apply** to confirm the change.

Fixed IP Address (EWAN)



The screenshot shows the 'Configuration' interface with the 'WAN Port' section selected. Under 'Parameters', the 'Main Port' is set to 'EWAN', the 'Protocol' is set to 'Fixed IP Address', and the 'IP Address' field contains '255.255.255.0'. Other fields include 'Netmask' (255.255.255.0), 'Gateway' (empty), 'Obtain DNS Automatically' (unchecked), and 'Primary DNS / Secondary DNS' (168.95.1.1 / 168.95.192.1). An 'Apply' button is visible at the bottom.

IP Address: Enter your fixed IP address.

Netmask: User can change it to others such as 255.255.255.128. Type the Netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

Click **Apply** to confirm the settings.

Pure Bridge (EWAN)

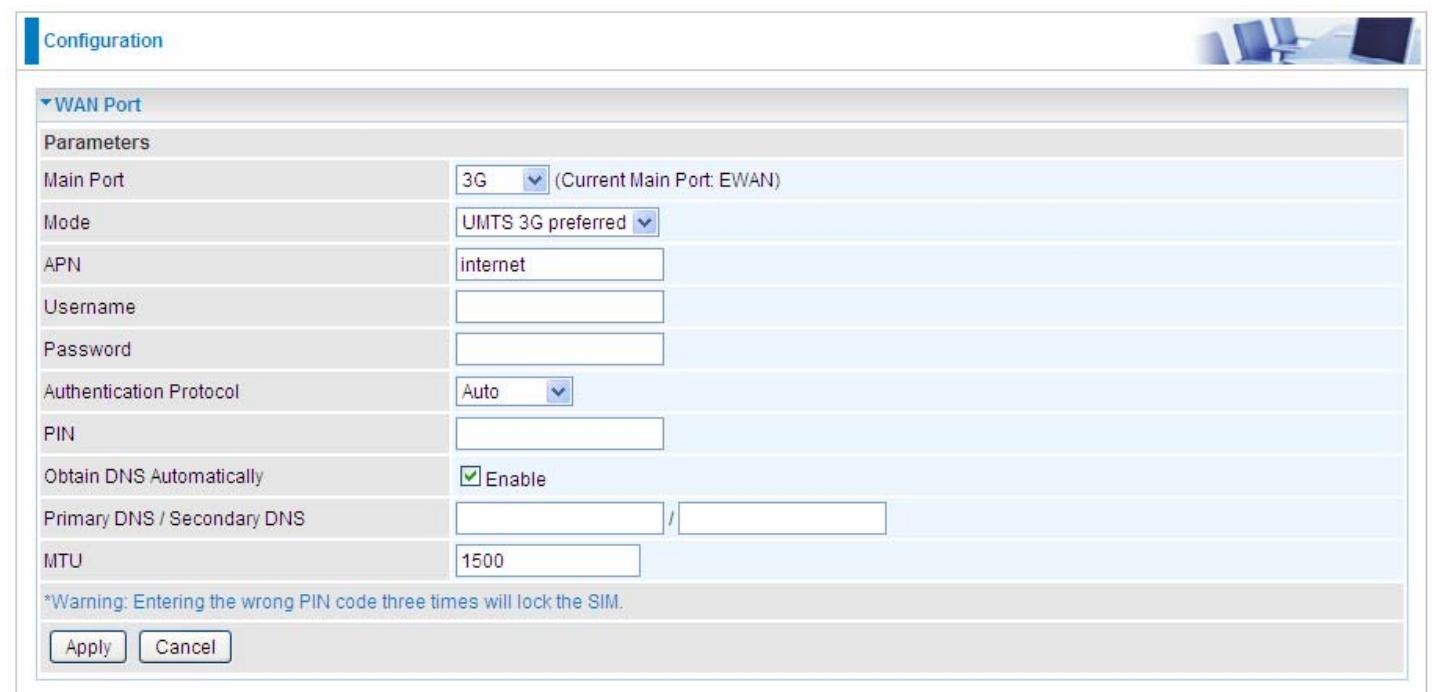


The screenshot shows the 'Configuration' tab selected in the top navigation bar. Under the 'WAN Port' section, the 'Main Port' is set to 'EWAN' (Current Main Port: 3G) and the 'Protocol' is set to 'Pure Bridge'. An 'Apply' button is visible at the bottom left.

Main Port: Select EWAN as the profile port.

WAN – Main Port (3G)

The setup of 3G is simplified by the web browser-based configuration. It is easy for you to access to the Internet wherever a 3G connection is available.



The screenshot shows the 'Configuration' tab selected. Under the 'WAN Port' section, the 'Main Port' is set to '3G' (Current Main Port: EWAN). Other settings include 'Mode: UMTS 3G preferred', 'APN: internet', 'Username' and 'Password' fields, 'Authentication Protocol: Auto', 'PIN' field, 'Obtain DNS Automatically: Enable', 'Primary DNS / Secondary DNS' fields, and 'MTU: 1500'. A warning message at the bottom states: '*Warning: Entering the wrong PIN code three times will lock the SIM.' An 'Apply' and 'Cancel' button are at the bottom.

Mode: There are 5 options of phone service standards: GSM 2G only, UMTS 3G only, GSM 2G preferred, UMTS 3G preferred, and Automatic. If you are uncertain what services are available to you, and then please select Automatic.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. Some 3G operators use the APN 'internet' for their portal. The default value is "internet".

Username/Password: Enter the username and password provided by your ISP.

Authentication Protocol: Default is Auto. Please consult your ISP on whether to use PAP, CHAP or MSCHAP.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain

systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/service provider.

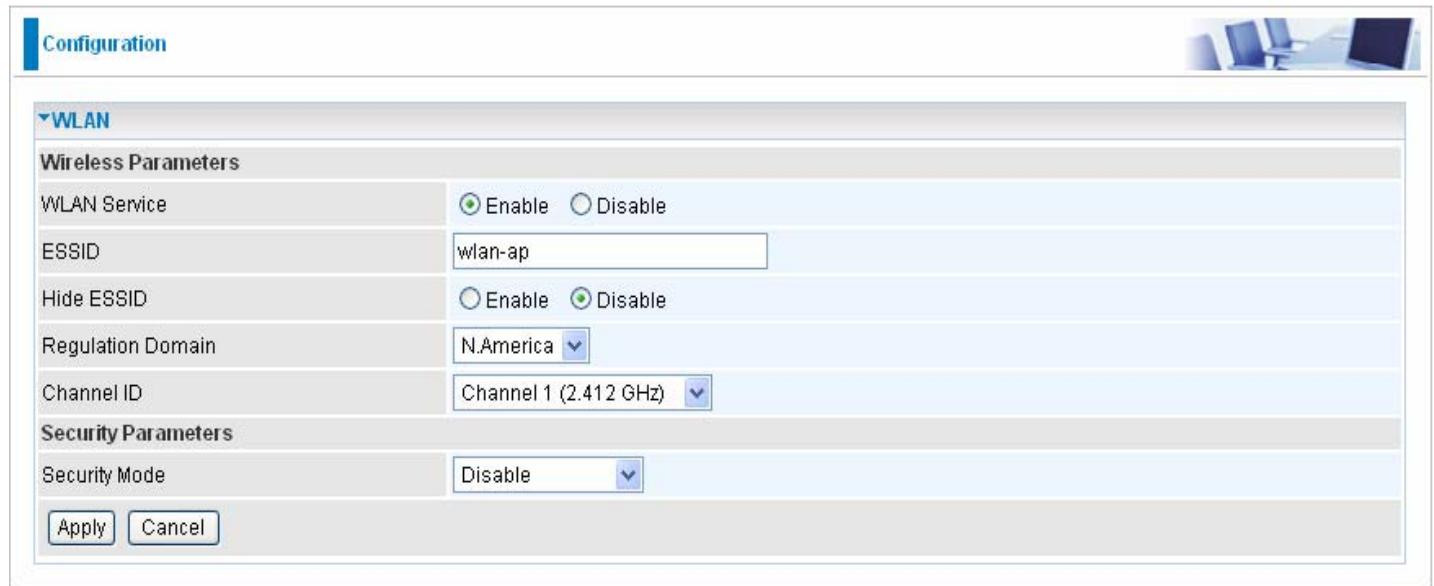
Obtain DNS Automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to enable this function.

Primary DNS/Secondary DNS: Enter the primary and secondary DNS.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Click Apply to confirm the settings.

WLAN



The screenshot shows the 'WLAN' configuration page. The 'Wireless Parameters' section contains fields for WLAN Service (set to Enable), ESSID (wlan-ap), Hide ESSID (set to Disable), Regulation Domain (N.America), and Channel ID (Channel 1 (2.412 GHz)). The 'Security Parameters' section shows Security Mode set to Disable. At the bottom are 'Apply' and 'Cancel' buttons.

Wireless Parameters

WLAN Service: Default setting is set to Enable. If you do not have any wireless, select Disable.

ESSID: The ESSID is a unique name of a wireless access point (AP) used to distinguish one from another. For security purpose, change the default wlan-ap to a unique ID name that is already built into the router wireless interface. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

Note: *It is case sensitive and must not exceed 32 characters.*

Hide ESSID: It is used to broadcast its ESSID on the network so that when a wireless client searches for a network, the router can be discovered and recognized. Default setting is Disable.

- **Enable:** Select Enable if you do not want broadcast your ESSID. When select Enable, the ESSID will be hided in stead of broadcasting, thus when wireless client searches for this AP, failure occurs. This ESSID (AP) will be invisible to you. In this case, if you want to join this wireless network, enter the exactly ESSID manually and some security settings.
- **Disable:** When Disable is selected, the router will broadcast the ESSID to allow anybody with a wireless client to be able to identify the Access Point (AP) of your router. Select the specific ESSID scanned, with some security settings, you will join this wireless network.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection channel ID that you would like to use.

Note: *Wireless performance may degrade if the selected channel ID is already being occupied by other AP(s).*

Security Parameters

Security Mode: You can disable or enable the function with WPA or WEP to protect the wireless network. The default mode of wireless security is Disable.

Click Apply to confirm the settings.

Security Mode

WPA or WPA2

Security Parameters	
Security Mode	WPA
RADIUS / 802.1x	<input type="checkbox"/> Enable
WPA Shared Key	<input type="text"/>
Group Key Renewal	3600 seconds

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network.

RADIUS/802.1x: Select Whether to enable or disable the RADIUS Service.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

If you want to enable the RADIUS service, check Enable and then do the following settings.

Security Parameters	
Security Mode	WPA
RADIUS / 802.1x	<input checked="" type="checkbox"/> Enable
Group Key Renewal	3600 seconds
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Shared Secret	<input type="text"/>

RADIUS Server IP Address: Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here. Default value is 1812.

RADIUS Shared Secret: Enter the password of RADIUS authentication server.

WPA/WPA2 Pre-Shared Key

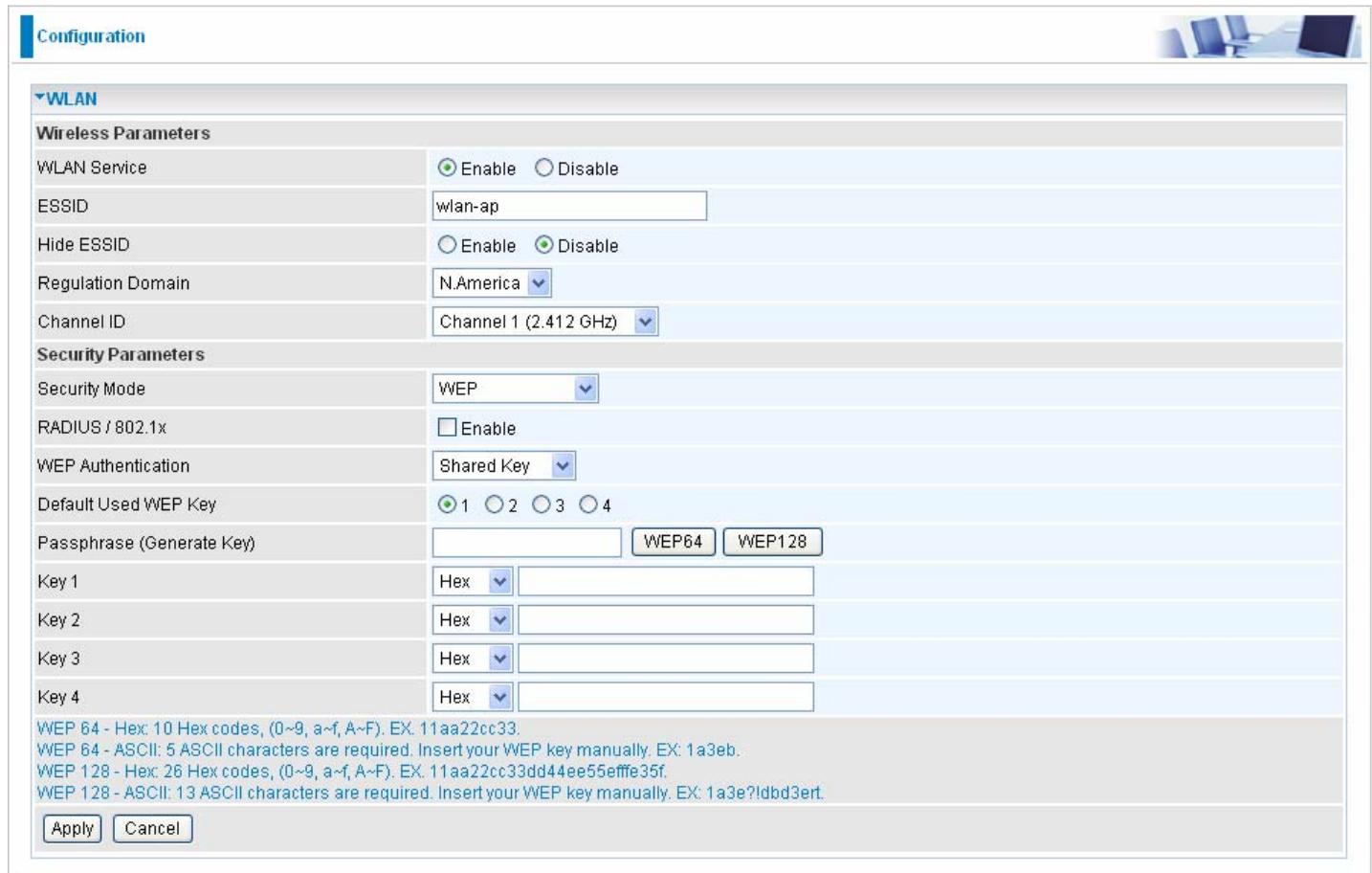
Security Parameters	
Security Mode	WPA/WPA2-PSK
WPA Shared Key	<input type="text"/>
Group Key Renewal	3600 seconds

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

WEP



Configuration

WLAN

Wireless Parameters

WLAN Service: Enable Disable

ESSID: wlan-ap

Hide ESSID: Enable Disable

Regulation Domain: N.America

Channel ID: Channel 1 (2.412 GHz)

Security Parameters

Security Mode: WEP

RADIUS / 802.1x: Enable

WEP Authentication: Shared Key

Default Used WEP Key: 1 2 3 4

Passphrase (Generate Key): WEP64

Key 1: Hex

Key 2: Hex

Key 3: Hex

Key 4: Hex

WEP 64 - Hex: 10 Hex codes, (0~9, a~f, A~F). EX. 11aa22cc33.

WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.

WEP 128 - Hex: 26 Hex codes, (0~9, a~f, A~F). EX. 11aa22cc33dd44ee55efffe35f.

WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?lbd3ert.

Apply Cancel

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network.

RADIUS/802.1x: Choose this box enable RADIUS/802.1x authentication protocol for boosting up WLAN Security.

WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are 3 options to select from: **Open System**, **Share Key** and **Both**.

Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX or ASCII style, 5 and 13 ASCII codes are required for WEP64 and WEP128 or 10 and 26 HEX codes are required for WEP64 and WEP128 respectively.

If you want to enable the RADIUS service, check Enable and then do the following settings.

Security Parameters	
Security Mode	WEP
RADIUS / 802.1x	<input checked="" type="checkbox"/> Enable
WEP Authentication	Open System
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Shared Secret	

WEP Authentication: If you enable **RADIUS/802.1x**, then the default **WEP Authentication** is **Open System**.

RADIUS Server IP Address: Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here. Default value is 1812.

RADIUS Shared Secret: Enter the password of RADIUS authentication server.

Advanced Configuration Mode

Status

The screenshot shows the 'Status' page of a router's configuration interface. It includes sections for Device Information, Physical Port Status, and WAN settings.

Device Information:

Model Name	BIPAC 7800GZ
Host Name	home.gateway
System Up-Time	45 min(s)
Current Time	Thu Sep 20 12:30:17 2012
Software Version	1.06g
MAC Address	00:04:ed:44:6d:c0

Physical Port Status:

Ethernet	✓
ADSL	✗
3G	✗
EWAN	✓
Wireless	✓

WAN:

Port	Protocol	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
EWAN	Dynamic	<input type="button" value="Release"/> <input type="button" value="Renew"/>	Up	172.16.1.204	255.255.255.0	172.16.1.254	172.16.1.254

Device Information

Model Name: Displays the model name.

Host Name: Provide a name for the router for identification purposes. Host Name lets you change the router name.

System Up-Time: Records system up-time.

Current time: Set the current time. See the Time Zone section for more information.

Hardware Version: Device version.

Software Version: Firmware version.

MAC Address: The LAN MAC address.

Physical Port Status

Port Status: User can look up to see if they are connected to Ethernet, WAN and Wireless.

WAN

Port: Name of the WAN connection, ADSL, EWAN or 3G.

Protocol: the current protocol used for the connection.

Operation: The current status in WAN interface.

Connection: The current connection status.

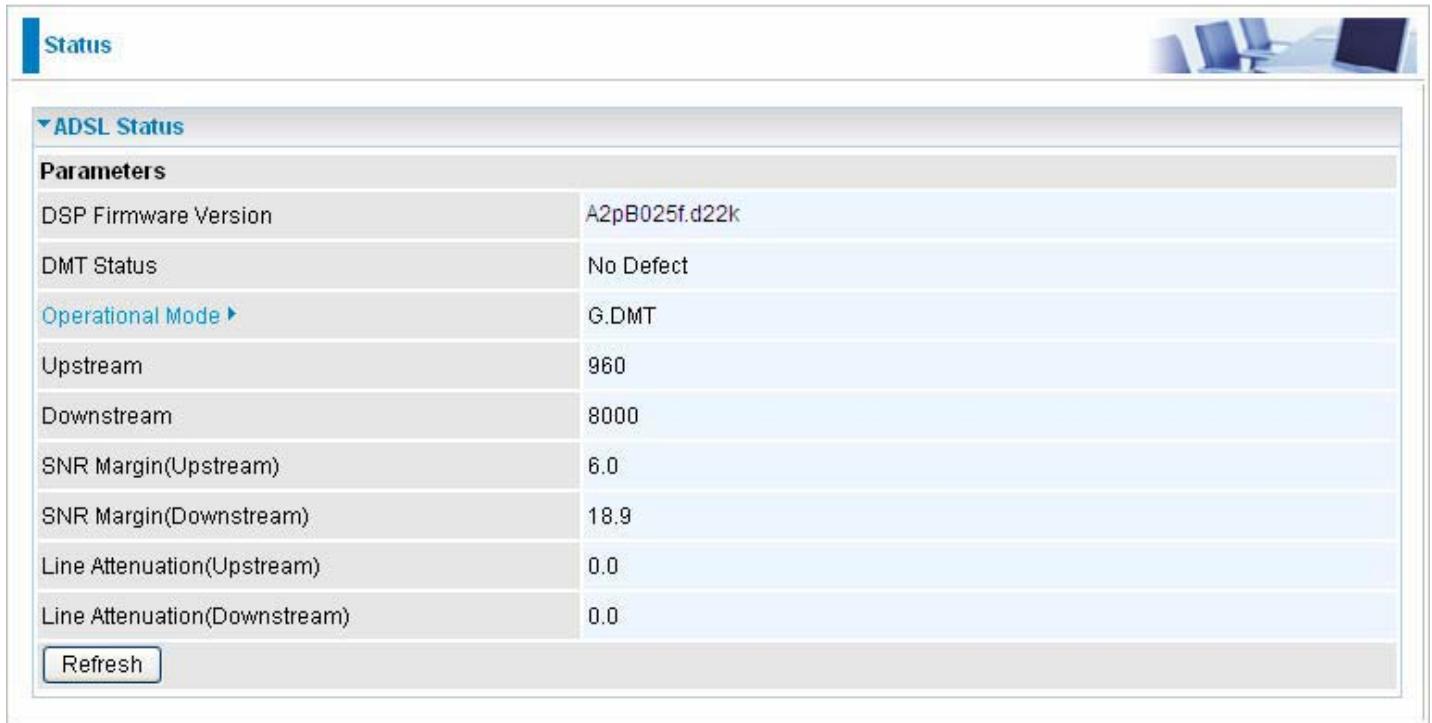
IP Address: WAN port IP address.

Netmask: WAN port IP subnet mask.

Gateway: The IP address of the default gateway.

Primary DNS: The IP address of the primary DNS server.

ADSL Status



The screenshot shows a web-based interface for monitoring ADSL status. At the top, a blue header bar contains the word 'Status'. Below this is a table with the following data:

Parameters	
DSP Firmware Version	A2pB025f.d22k
DMT Status	No Defect
Operational Mode ▶	G.DMT
Upstream	960
Downstream	8000
SNR Margin(Upstream)	6.0
SNR Margin(Downstream)	18.9
Line Attenuation(Upstream)	0.0
Line Attenuation(Downstream)	0.0

At the bottom left of the table is a 'Refresh' button.

DSP Firmware Version: DSP code version.

DMT Status: Current DMT Status.

Operational Mode: Displays the ADSL state when the connect mode is set to AUTO. Click Operational Mode link to go to the ADSL Mode configuration page. Click Operational Mode to go to [ADSL Mode](#) configuration page to configure ADSL mode.

Upstream: Upstream rate.

Downstream: Downstream rate.

SNR Margin (Upstream): This shows the SNR margin for upstream rate.

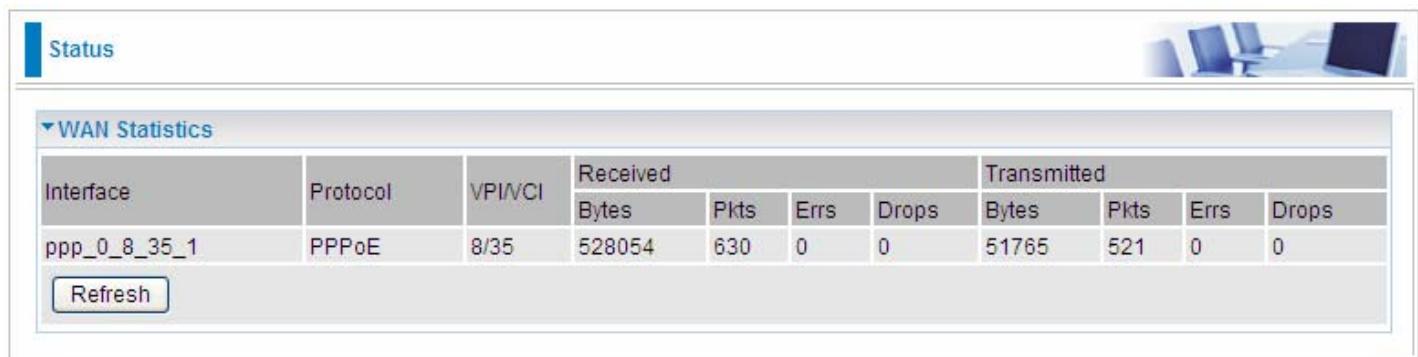
SNR Margin (Downstream): This shows the SNR margin for downstream rate.

Line Attenuation (Upstream): This is attenuation of signal in upstream.

Line Attenuation (Downstream): This is attenuation of signal in downstream.

Refresh: Click Refresh button to reset the statistics value of Upstream/Downstream rate.

WAN Statistics



Interface	Protocol	VPI/VCI	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ppp_0_8_35_1	PPPoE	8/35	528054	630	0	0	51765	521	0	0
<input type="button" value="Refresh"/>										

Interface: the name of the WAN Connection

Protocol: the protocol the WAN Connection adopt

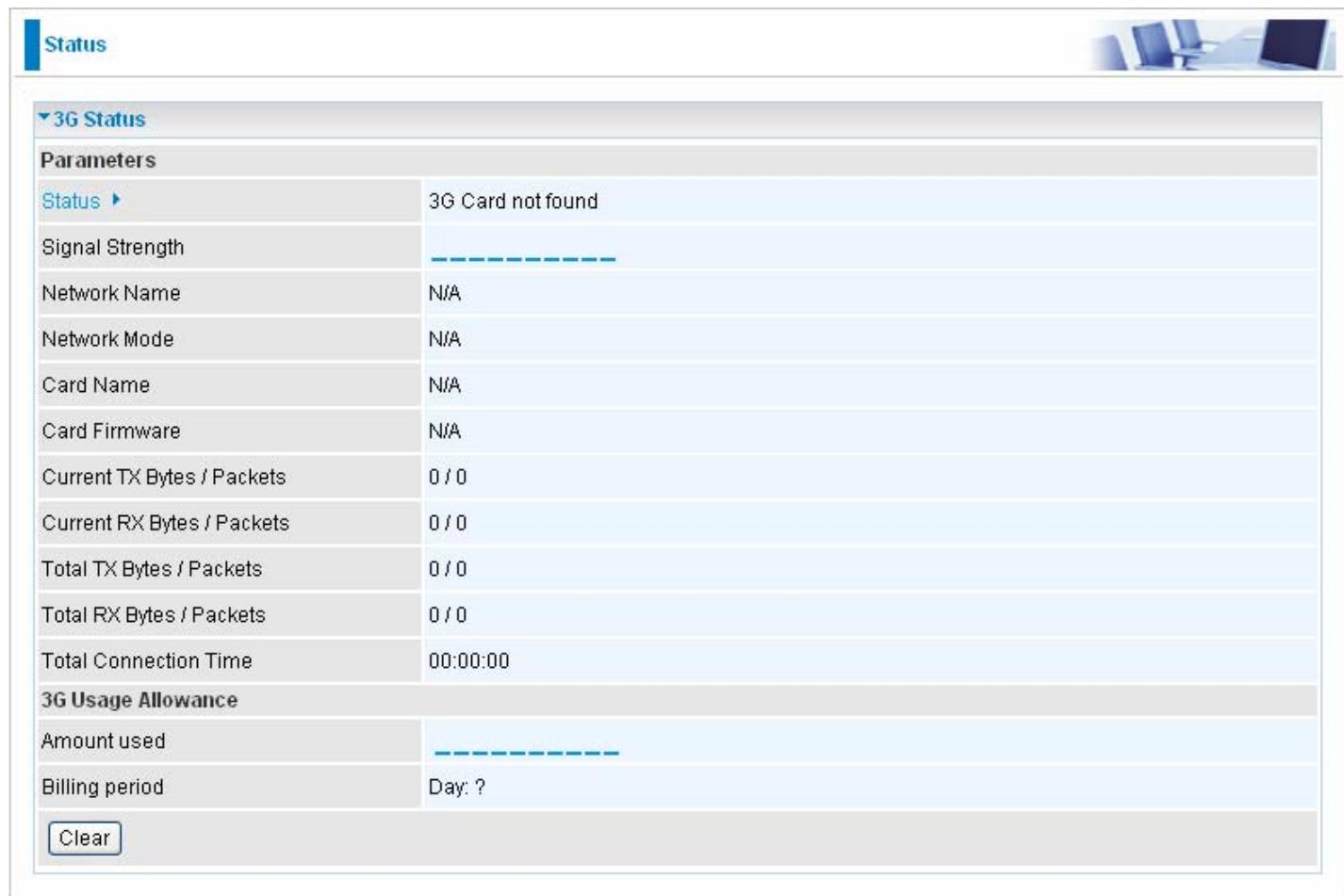
VPI/VCI: Virtual Path Identifier and Virtual Channel Identifier of the WAN Connection, it is provided by ISP.

Received: Include received Bytes, Pkts, Errs and Drops.

Transmitted: Include transmitted Bytes, Pkts, Errs and Drops.

Refresh: Click Refresh button to reset the statistics value of Received / Transmitted.

3G Status



3G Status	
Parameters	
Status	3G Card not found
Signal Strength	<div style="width: 100px; height: 10px; background-color: #ccc; border: 1px solid #ccc; margin-bottom: 5px;"></div>
Network Name	N/A
Network Mode	N/A
Card Name	N/A
Card Firmware	N/A
Current TX Bytes / Packets	0 / 0
Current RX Bytes / Packets	0 / 0
Total TX Bytes / Packets	0 / 0
Total RX Bytes / Packets	0 / 0
Total Connection Time	00:00:00
3G Usage Allowance	
Amount used	<div style="width: 100px; height: 10px; background-color: #ccc; border: 1px solid #ccc; margin-bottom: 5px;"></div>
Billing period	Day: ?
Clear	

Status: The current status of the 3G card. Click [Status](#) to go to 3G configuration page.

Signal Strength: The signal strength bar indicates current 3G signal strength.

Network Name: The network name that the device is connected to.

Network Mode: The current operation mode in 3G card, it depends on service provider and card's limitation. It may be UMTS(3G), GPRS, EDGE, or GSM .

Card Name: The name of the 3G card.

Card Firmware: The current firmware for the 3G card.

Current TX Bytes / Packets: The statistics of transmission, count for this call.

Current RX Bytes / Packets: The statistics of receive, count for this call.

Total TX Bytes / Packets: The statistics of transmission, count from system ready.

Total RX Bytes / Packets: The statistics of receive, count from system ready.

Total Connection Time: The statistics of the connection time since system is ready.

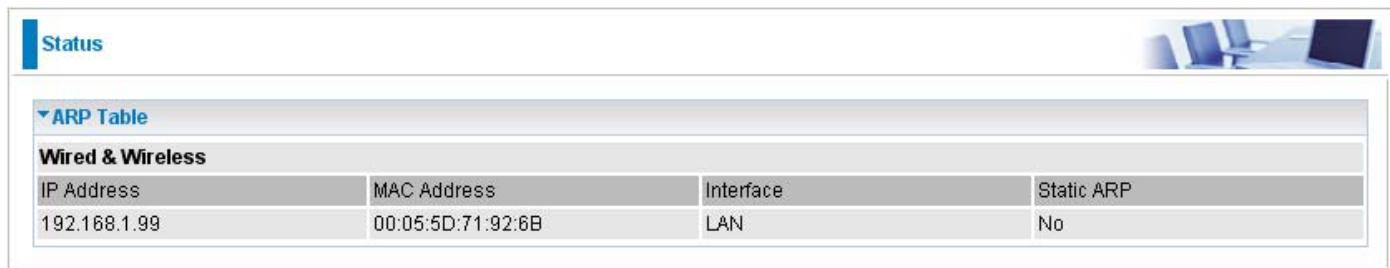
Amount used: the amount that have been used in 3G

Billing period: the remaining days before the billing terminated day.

Clear: Click Clear button to reset the statistics value of Total TX/RX.

ARP Table

This table stores mapping information that the device uses to find the Layer 2 Media Access Control (MAC) address that corresponds to the Layer 3 IP address of the device via the Address Resolution Protocol (ARP) feature.



ARP Table			
Wired & Wireless			
IP Address	MAC Address	Interface	Static ARP
192.168.1.99	00:05:5D:71:92:6B	LAN	No

IP Address: Shows the IP Address of the device that the MAC address maps to.

MAC Address: Shows the MAC address that is corresponded to the IP address of the device it is mapped to.

Interface: Shows the interface name (on the router) that this IP address connects to.

Static ARP: Shows the status of static ARP.

DHCP Table

The DHCP Table lists the DHCP lease information for all IP addresses assigned by the DHCP server in the device.



The screenshot shows a web-based interface for managing a DHCP table. At the top, there is a blue header bar with the word 'Status' on the left and a small graphic of three computer monitors on the right. Below this is a navigation menu with a blue arrow icon and the text '▼ DHCP Table'. Under 'Leased Table', there is a table with the following data:

IP Address	MAC Address	Client Host Name	Register Information
192.168.1.100	00:05:5d:6a:58:d2	chris-7c4c197a4	Remains 23:08:29

IP Address: The IP address which is assigned to the host with this MAC address.

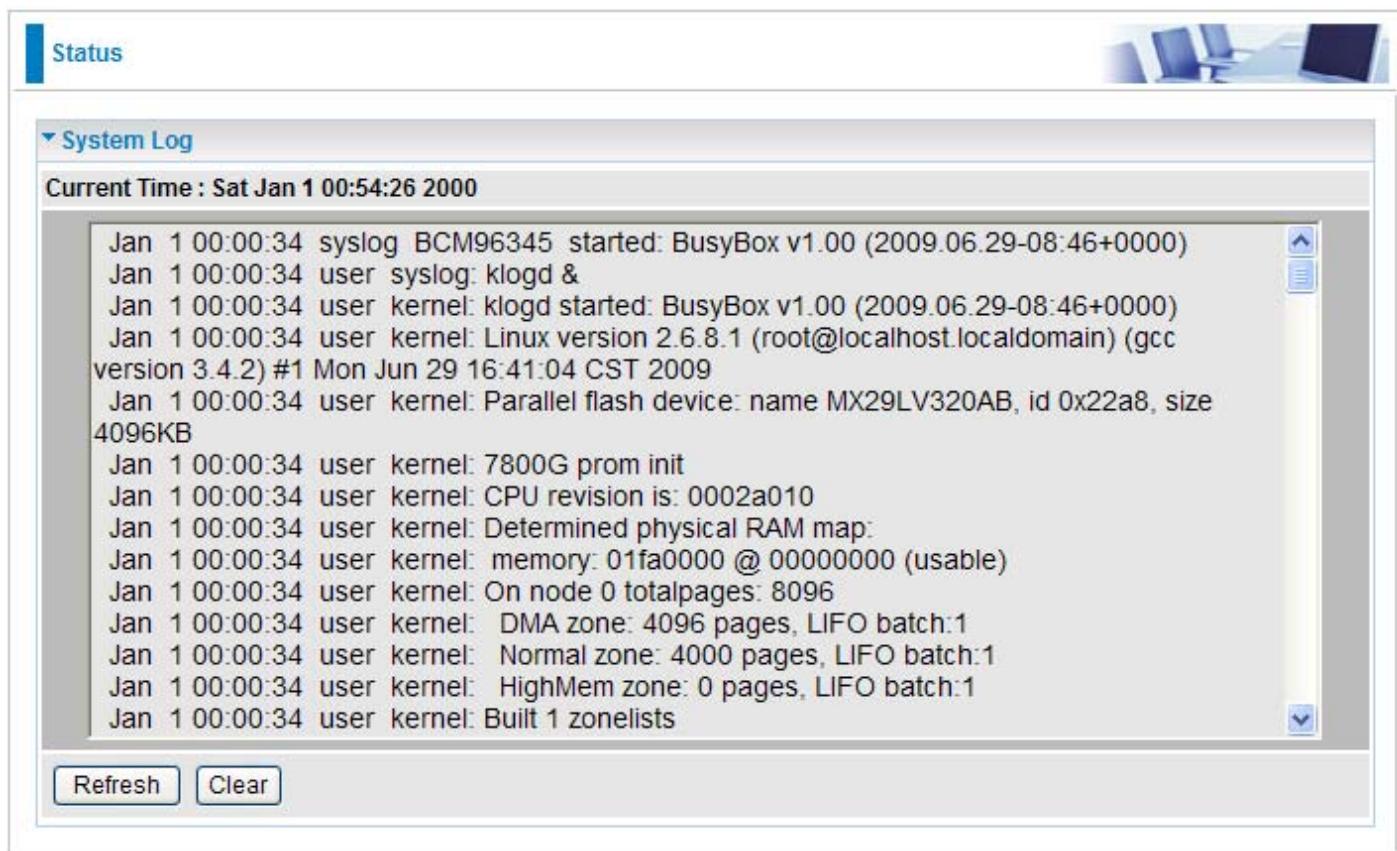
MAC Address: The MAC Address of internal dhcp client host.

Client Host Name: The Host Name of internal dhcp client.

Register Information: Shows the information provided during registration.

System Log

Display system logs accumulated up to the present time. You can trace its historical information with this function.



The screenshot shows a 'Status' interface with a 'System Log' section. The log output is as follows:

```
Jan 1 00:00:34 syslog BCM96345 started: BusyBox v1.00 (2009.06.29-08:46+0000)
Jan 1 00:00:34 user syslog: klogd &
Jan 1 00:00:34 user kernel: klogd started: BusyBox v1.00 (2009.06.29-08:46+0000)
Jan 1 00:00:34 user kernel: Linux version 2.6.8.1 (root@localhost.localdomain) (gcc
version 3.4.2) #1 Mon Jun 29 16:41:04 CST 2009
Jan 1 00:00:34 user kernel: Parallel flash device: name MX29LV320AB, id 0x22a8, size
4096KB
Jan 1 00:00:34 user kernel: 7800G prom init
Jan 1 00:00:34 user kernel: CPU revision is: 0002a010
Jan 1 00:00:34 user kernel: Determined physical RAM map:
Jan 1 00:00:34 user kernel: memory: 01fa0000 @ 00000000 (usable)
Jan 1 00:00:34 user kernel: On node 0 totalpages: 8096
Jan 1 00:00:34 user kernel: DMA zone: 4096 pages, LIFO batch:1
Jan 1 00:00:34 user kernel: Normal zone: 4000 pages, LIFO batch:1
Jan 1 00:00:34 user kernel: HighMem zone: 0 pages, LIFO batch:1
Jan 1 00:00:34 user kernel: Built 1 zonelists
```

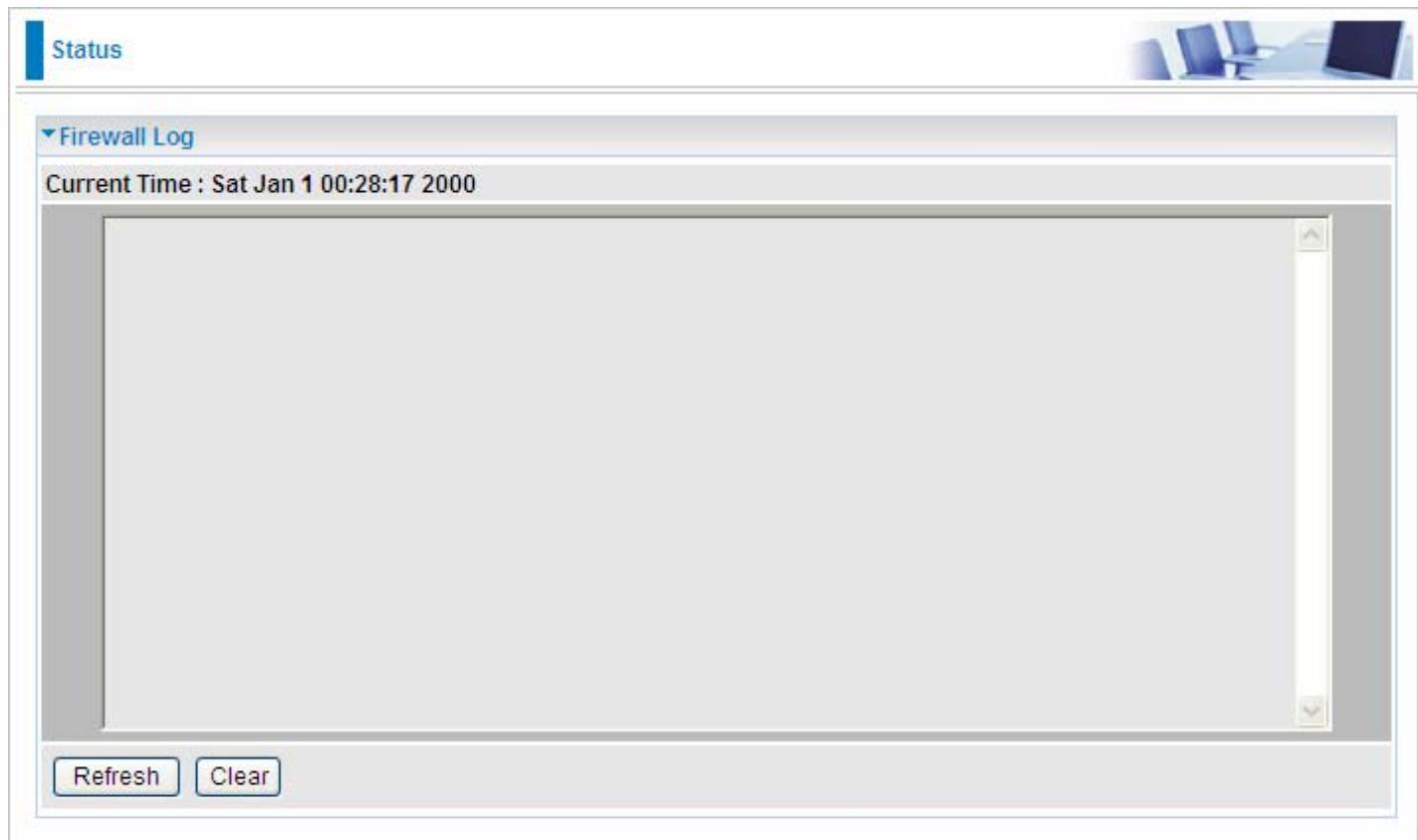
At the bottom of the log window are two buttons: 'Refresh' and 'Clear'.

Refresh: Click to update the system log.

Clear: Click to clear the current log from the screen.

Firewall Log

Firewall Log display log information of any unexpected action with your firewall settings. This page displays the router's Firewall Log entries. The log shows log entries when you have enabled Intrusion Detection or Block WAN PING in the **Configuration – Firewall** section of the interface. Please see the **Firewall** section of this manual for more details on how to enable Firewall logging.



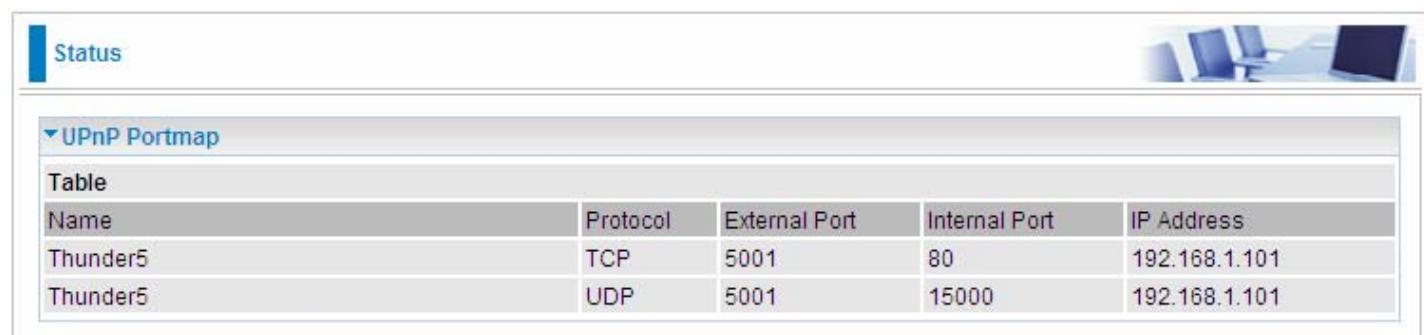
The screenshot shows the 'Firewall Log' section of a router's configuration interface. At the top, there is a 'Status' bar. Below it, a section titled 'Firewall Log' is expanded. It displays the current time as 'Sat Jan 1 00:28:17 2000'. The main area is a large, empty window with scroll bars on the right and bottom. At the bottom of this window, there are two buttons: 'Refresh' and 'Clear'.

Refresh: Click to update the firewall log.

Clear: Click to clear the current log from the screen.

UPnP Portmap

The UPnP Portmap table displays the IP address of each UPnP device that is accessing the router. It also shows the ports (Internal and External) that device has opened.



The screenshot shows the 'UPnP Portmap' section of a router's configuration interface. At the top, there is a 'Status' bar. Below it, a section titled 'UPnP Portmap' is expanded. A table titled 'Table' is displayed, showing the following data:

Name	Protocol	External Port	Internal Port	IP Address
Thunder5	TCP	5001	80	192.168.1.101
Thunder5	UDP	5001	15000	192.168.1.101

IPSec Status

The IPSec Table provides administrators with detailed information regarding the configured IPSec VPN Connections.

IPSec Status					
VPN Tunnels					
Name	Active	Local Subnet	Remote Subnet	Remote Gateway	SA
<input type="button" value="Refresh"/>					

Name: The name you assigned to the particular VPN entry.

Active: Whether the VPN Connection is currently Active.

Local Subnet: The local IP Address or Subnet used.

Remote Subnet: The Subnet of the remote site.

Remote Gateway: The Remote Gateway IP address.

SA: The Security Association for this VPN entry.

Refresh: click this button to view the latest status.

VRRP Status

The VRRP Status displays information of current status and current master of VRRP.

VRRP Status	
Parameters	
Current Status	
Current Master	

Current Status: Show VRRP current status, Master or Backup.

Current Master: Show the IP address of current master.

Configuration

When you click this item, the column will expand to display the sub-items that will allow you to further configure your router.

[LAN](#), [WAN](#), [System](#), [Firewall](#), [VPN](#), [QoS](#), [Virtual Server](#), [Wake on LAN](#), [Certificate](#), [Time Schedule](#) and [Advanced](#).

The function of each configuration sub-item is described in the following sections.

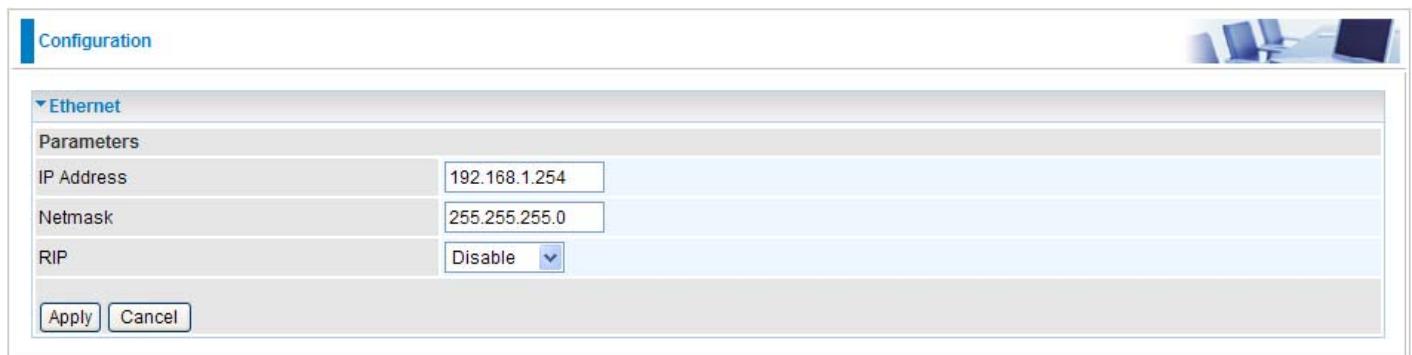
LAN - Local Area Network

A Local Area Network (LAN) is a shared communication system network where many computers are connected. This type of network is area defined and is usually limited to a confined region within a building or just within the same storey of a building.

There are 7 items within the LAN section: [Ethernet](#), [IP Alias](#), [Wireless](#), [Wireless Security](#), [WPS](#), [DHCP Server](#) and [VRRP](#).

Ethernet

The router supports more than one Ethernet IP addresses in the LAN that supports multiple internet access at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.1.254.



IP Address	192.168.1.254
Netmask	255.255.255.0
RIP	Disable

IP Address: The default IP on this router.

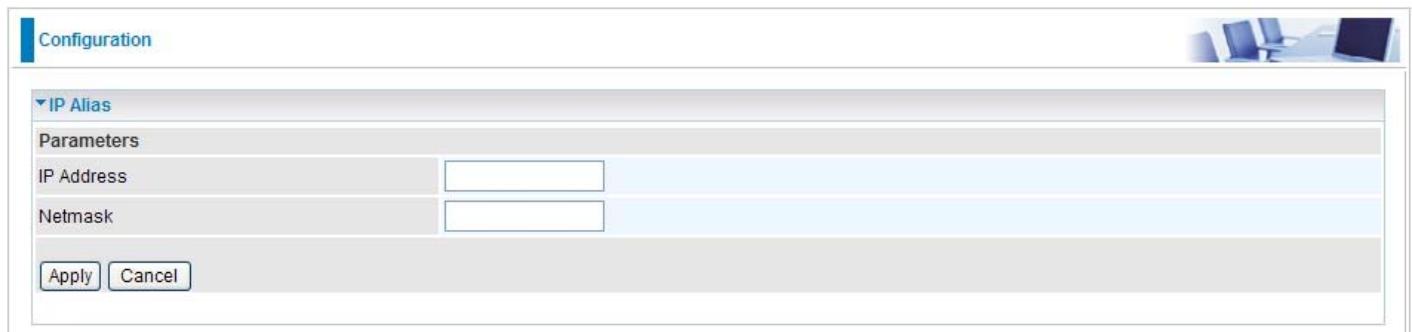
Netmask: The default subnet mask on this router.

RIP: RIP v1, RIP v2 and RIP v1+v2. Check to enable RIP function.

Click Apply to confirm the settings.

IP Alias

This function allows the addition an IP alias to the network interface. It further allows user the flexibility to assign a specific function to use this IP.



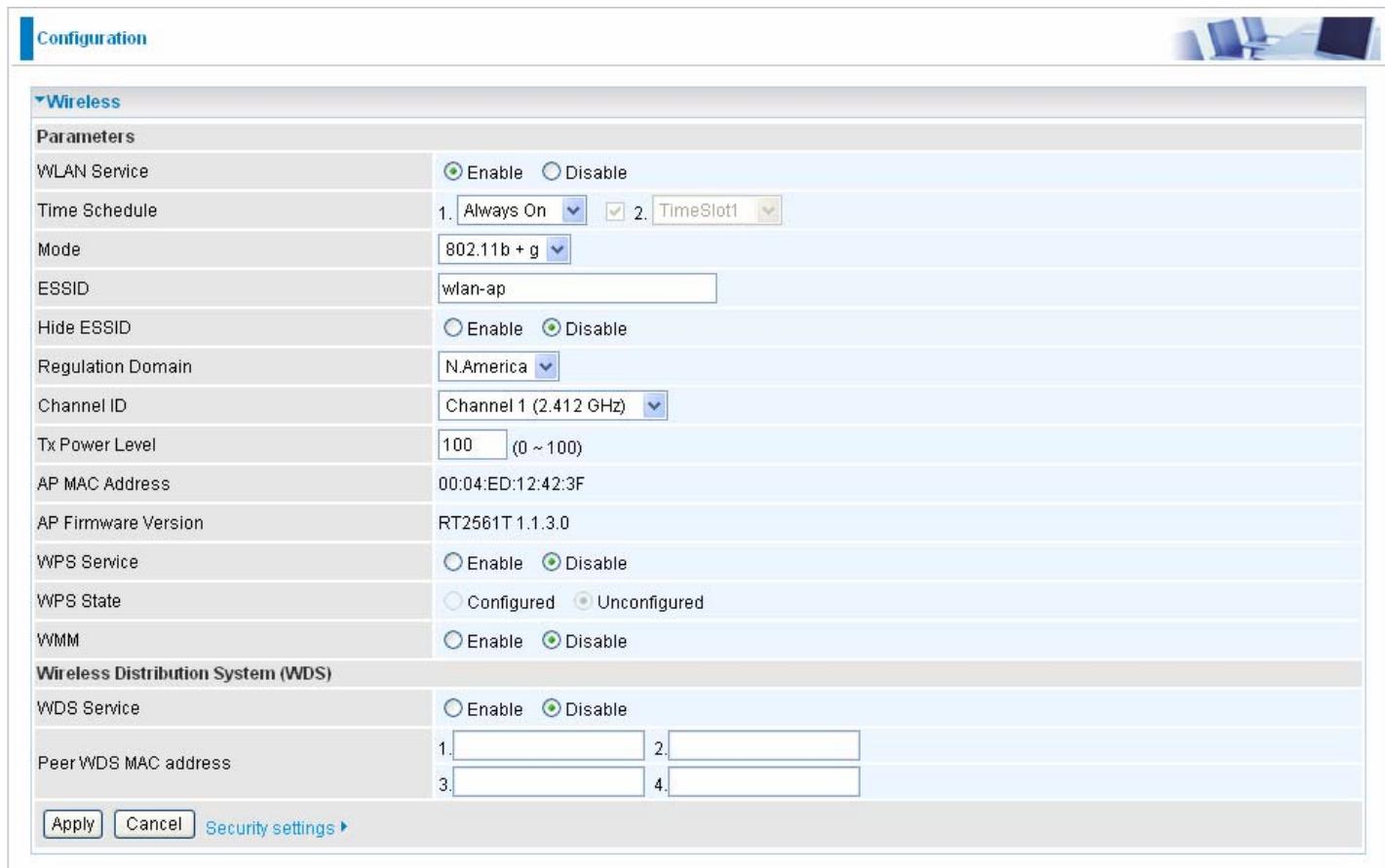
IP Address	
Netmask	

IP Address: Enter the IP address to be added to the network.

Netmask: Specify a subnet mask for the IP to be added.

Click Apply to confirm the settings.

Wireless



The screenshot shows the 'Wireless' configuration page. At the top, there is a 'Configuration' tab and a small graphic of a computer monitor. The main area is titled 'Wireless' and contains several configuration sections:

- Parameters**
 - WLAN Service: Radio button for 'Enable' (selected) or 'Disable'.
 - Time Schedule: A dropdown menu with 'Always On' (selected) and 'TimeSlot1' as options.
 - Mode: A dropdown menu set to '802.11b + g'.
 - ESSID: A text input field containing 'wlan-ap'.
 - Hide ESSID: Radio button for 'Enable' (selected) or 'Disable'.
 - Regulation Domain: A dropdown menu set to 'N.America'.
 - Channel ID: A dropdown menu set to 'Channel 1 (2.412 GHz)'.
 - Tx Power Level: A text input field with '100' and '(0 ~ 100)'.
 - AP MAC Address: A text input field showing '00:04:ED:12:42:3F'.
 - AP Firmware Version: Text showing 'RT2561T 1.1.3.0'.
 - WPS Service: Radio button for 'Enable' (selected) or 'Disable'.
 - WPS State: Radio button for 'Configured' (selected) or 'Unconfigured'.
 - WMM: Radio button for 'Enable' (selected) or 'Disable'.
- Wireless Distribution System (WDS)**
 - WDS Service: Radio button for 'Enable' (selected) or 'Disable'.
 - Peer WDS MAC address: A text input field with four sections: 1., 2., 3., and 4., each containing a blank line.

At the bottom are 'Apply', 'Cancel', and 'Security settings' buttons.

Parameters

WLAN Service: Default setting is set to Enable. If you do not have any wireless, select Disable.

Time Schedule: A self defined time period. You may specify a time schedule for your prioritization policy.

Here we provide two groups of **Time Schedule** setting. You can flexibly set the time you want the wireless connection works.

If you select **Always On** in group1, then the group2 is disabled.

While if you select any other item from the group1 drop-down menu, the group2 will be activated.

Select the timeslot you want, then the wireless will work according to the time of the two time schedule settings. That is to say you can flexibly set the time the wireless works.

For setup and detail, refer to Time Schedule section.

Mode: The default setting is 802.11b+g. From the drop-down manual, you can select 802.11b if you have only 11b card. If you have only 11g card, select 802.11g.

ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

Hide ESSID: This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

- **Enable:** Select Enable if you do not want broadcast your ESSID. When select Enable, the ESSID will be hidden instead of broadcasting, thus when wireless client searches for this AP, failure occurs. This ESSID(AP) will be invisible to you. In this case, if you want to join this wireless network, enter the exactly ESSID manually and some security settings.
- **Disable:** When Disable is selected, the router will broadcast the ESSID to allow anybody with a wireless client to be able to identify the Access Point (AP) of your router. Select the specific ESSID scanned, with some security settings, you will join this wireless network.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection channel ID that you would like to use.

Note: *Wireless performance may degrade if the selected channel ID is already being occupied by other AP(s).*

TX PowerLevel: It is a function that enhances the wireless transmitting signal strength. User may adjust this power level from minimum 0 up to maximum 100.

Note: *The Power Level maybe different in each access network user premise environment, choose the most suitable level for your network.*

AP MAC Address: It is a unique hardware address of the Access Point.

AP Firmware Version: The Access Point firmware version.

WPS Service: Select Enable if you would like to activate WPS service.

WPS State: This column allows you to set the status of the device wireless setting whether it has been configured or unconfigured. For WPS configuration please refer to the section on **Wi-Fi Network Setup** for detail.

WMM: This feature is used to control the prioritization of traffic according to 4 Access categories: Voice, Video, Best Effort and Background. Default is set to disable.

- **Enable:** Click to activate WMM feature.
- **Disable:** Click to deactivate WMM feature.

Wireless Distribution System (WDS)

It is a wireless access point mode that enables wireless link and communication with other access points. It is easy to install simply by defining the peer's MAC address of the connected AP. WDS takes advantages of the cost saving and flexibility which no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network. It can connect up to 4 wireless APs for extending cover range at the same time.

In addition, WDS also enhances its link connection security mode. Key encryption and channel must be the same for both access points.

WDS Service: The default setting is disabled. Check **Enable** radio button to activate this function.

1. **Peer WDS MAC Address:** It is the associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other.
2. **Peer WDS MAC Address:** It is the second associated AP's MAC Address.

3. **Peer WDS MAC Address:** It is the third associated AP's MAC Address.
4. **Peer WDS MAC Address:** It is the fourth associated AP's MAC Address.

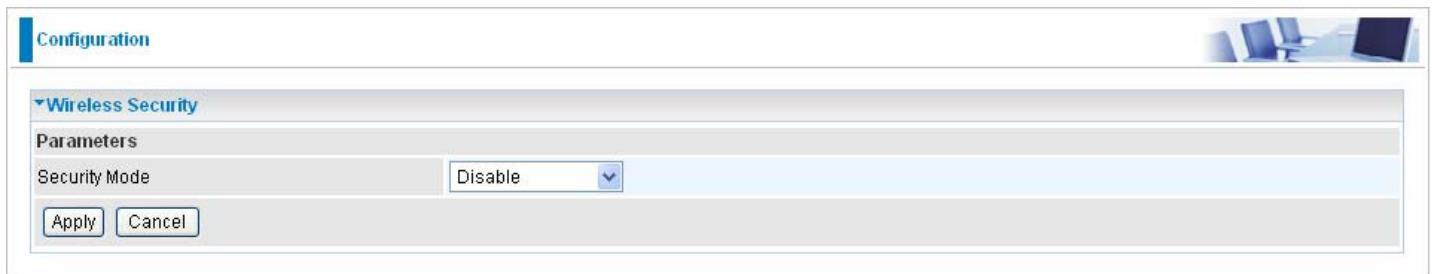
Note: For MAC Address, the format can be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Click Apply to confirm the settings.

You can click Security settings link next to Cancel button to go to Wireless Security screen (see **Wireless Security** section).

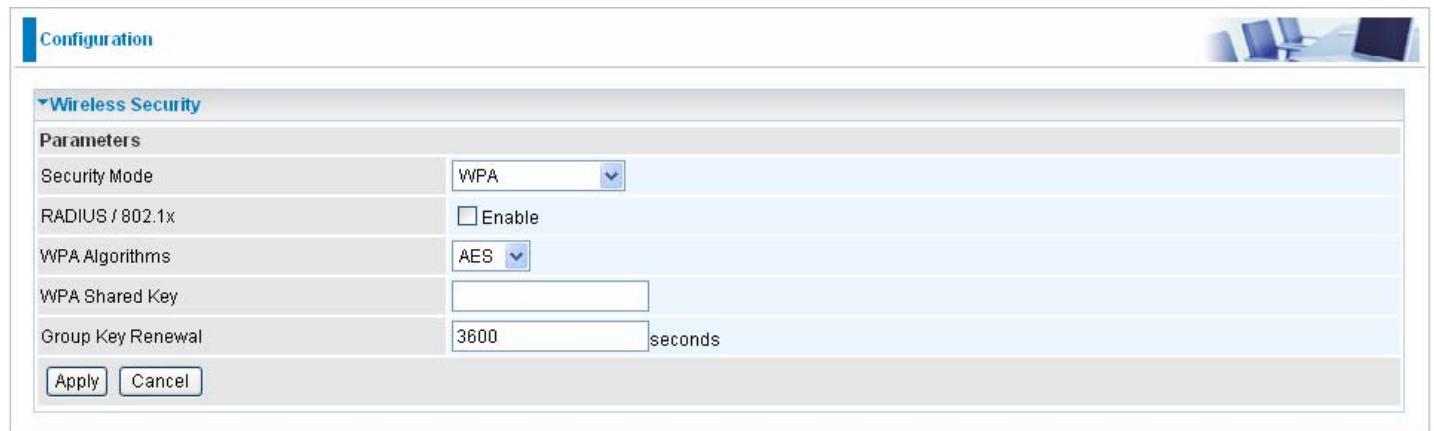
Wireless Security

You can disable or enable wireless security function using WPA or WEP for protecting wireless network. The default mode of wireless security is disabled.



WPA or WPA2

Here take **WPA** for example.



Security Mode: You can choose the type of security mode you want to apply from the drop-down menu.

RADIUS/802.1x: Select Whether to enable or disable the RADIUS Service.

WPA Algorithms: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol) which help to protect the wireless communication. The Default algorithm is AES.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

If you want to enable the RADIUS service, check Enable and then do the following settings.



Parameters	
Security Mode	WPA
RADIUS / 802.1x	<input checked="" type="checkbox"/> Enable
WPA Algorithms	AES
Group Key Renewal	3600 seconds
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Shared Secret	

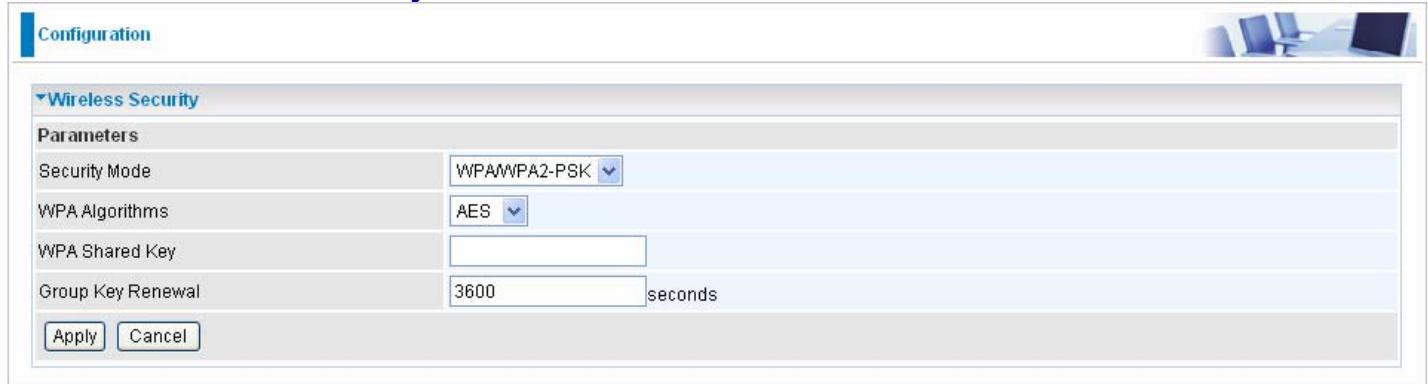
RADIUS Server IP Address: Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here. Default value is 1812.

RADIUS Shared Secret: Enter the password of RADIUS authentication server.

Click Apply to confirm the settings.

WPA / WPA2 Pre-Shared Key



Parameters	
Security Mode	WPA/WPA2-PSK
WPA Algorithms	AES
WPA Shared Key	
Group Key Renewal	3600 seconds

Security Mode: You can choose the type of security mode you want to apply from the drop-down menu.

WPA Algorithms: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol) which help to protect the wireless communication. The Default algorithm is AES.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

Click Apply to confirm the settings.

WEP

Configuration

Wireless Security

Parameters

Security Mode: WEP

RADIUS / 802.1x: Enable

WEP Authentication: Shared Key

Default Used WEP Key: 1 2 3 4

Passphrase (Generate Key):

Key 1: Hex

Key 2: Hex

Key 3: Hex

Key 4: Hex

WEP 64 - Hex: 10 Hex codes, (0~9, a~f, A~F). EX. 11aa22cc33.
WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.
WEP 128 - Hex: 26 Hex codes, (0~9, a~f, A~F). EX. 11aa22cc33dd44ee55efffe35f.
WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?l!dbd3ert.

Security Mode: Choose the type of security mode **WEP** from the drop-down menu.

RADIUS/802.1x: Choose this box enable RADIUS/802.1x authentication protocol for boosting up WLAN Security.

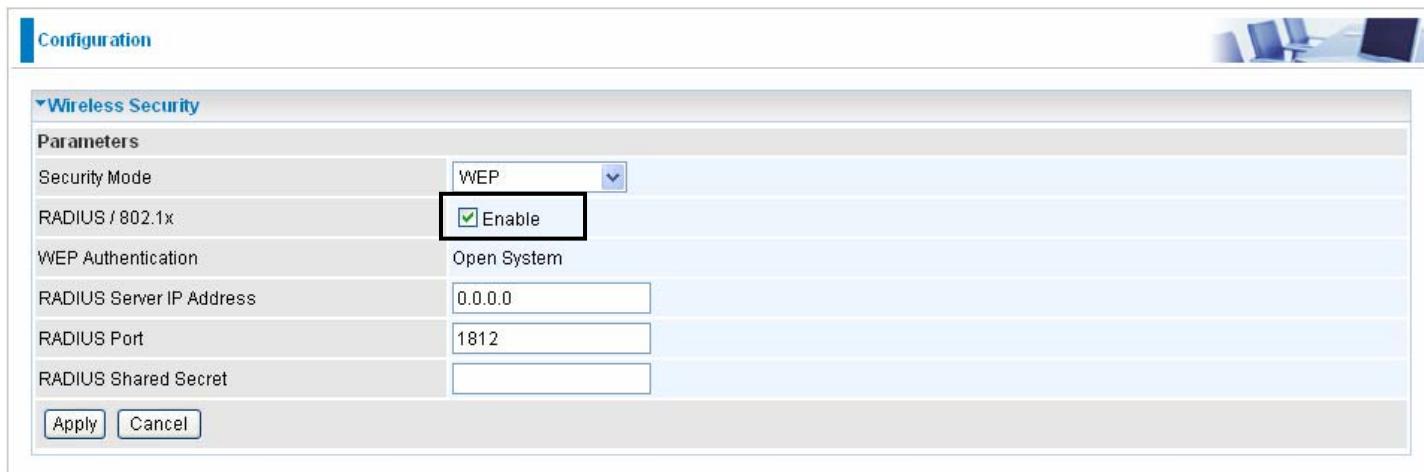
WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. There are 3 options to select from: **Open System**, **Shared Key** or **Both**.

Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX or ASCII style, 5 and 13 ASCII codes are required for WEP64 and WEP128 or 10 and 26 HEX codes are required for WEP64 and WEP128 respectively.

If you want to enable the RADIUS service, check Enable and then do the following settings.



The screenshot shows a configuration interface for 'Wireless Security' settings. The 'Parameters' section includes the following fields:

Security Mode	WEP
RADIUS / 802.1x	<input checked="" type="checkbox"/> Enable
WEP Authentication	Open System
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Shared Secret	[Redacted]

At the bottom are 'Apply' and 'Cancel' buttons.

WEP Authentication: If you enable **RADIUS/802.1x**, then the default **WEP Authentication** is **Open System**.

RADIUS Server IP Address: Enter the IP address of RADIUS authentication server.

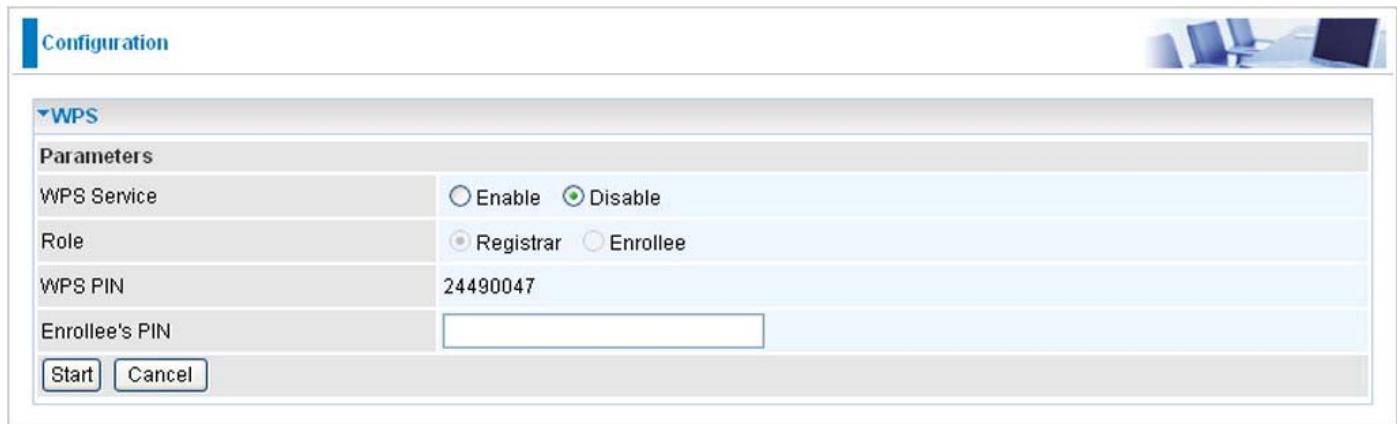
RADIUS Server Port: Enter the port number of RADIUS authentication server here. Default value is 1812.

RADIUS Shared Secret: Enter the password of RADIUS authentication server.

Click Apply to confirm the settings.

WPS

WPS (WiFi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN Method & PBC Method**.



The screenshot shows a 'Configuration' interface with a 'WPS' section. The 'Parameters' table contains the following data:

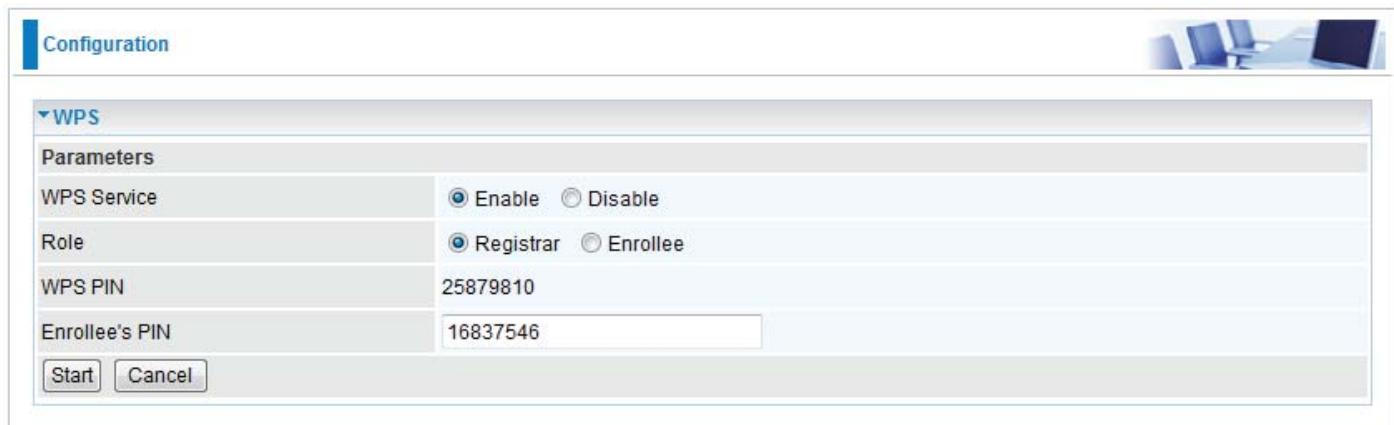
Parameters	
WPS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Role	<input checked="" type="radio"/> Registrar <input type="radio"/> Enrollee
WPS PIN	24490047
Enrollee's PIN	<input type="text"/>

At the bottom are 'Start' and 'Cancel' buttons.

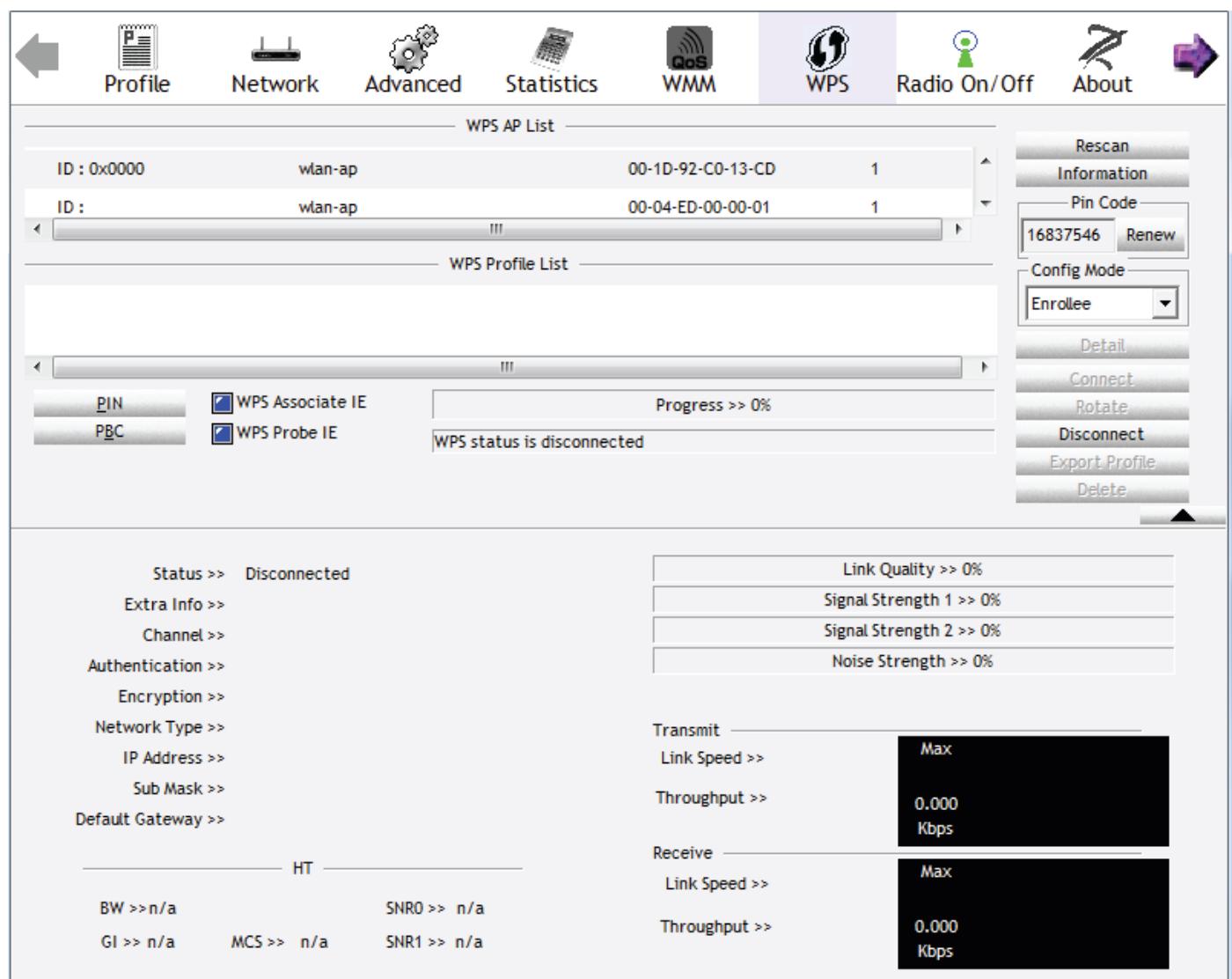
Wi-Fi Network Setup

PIN Method: Configure AP as Registrar

1. Jot down the client's Pin (eg. 16837546).



2. Enter the Enrollee's PIN number and then press Start.
3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Enrollee, press the WPS button on the top bar, select the AP (eg. wlan-ap) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.



4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar.

The screenshot shows a network configuration interface with the following sections:

- WPS AP List:** Displays two entries: "wlan-ap" with MAC address 00-1D-92-C0-13-CD and "wlan-ap" with MAC address 00-04-ED-38-F7-2E, both assigned to channel 1.
- WPS Profile List:** Shows a single profile named "wlan-ap". Under "PIN" and "PBC" options, checkboxes for "WPS Associate IE" and "WPS Probe IE" are selected. A progress bar indicates "Progress >> 100%" and the message "PIN - Get WPS profile successfully.".
- Status:** Lists network configuration details:
 - Status >> wlan-ap <-> 00-1D-92-C0-13-CD
 - Extra Info >> Link is Up [TxPower:100%]
 - Channel >> 1 <-> 2412 MHz; central channel : 3
 - Authentication >> Open
 - Encryption >> NONE
 - Network Type >> Infrastructure
 - IP Address >> 192.168.1.100
 - Sub Mask >> 255.255.255.0
 - Default Gateway >> 192.168.1.254
- Link Quality:** Shows signal strength levels:
 - Link Quality >> 100%
 - Signal Strength 1 >> 64%
 - Signal Strength 2 >> 34%
 - Noise Strength >> 26%
- Transmit:** Displays link speed and throughput data:
 - Link Speed >> 270.0 Mbps
 - Throughput >> 5.600 Kbps
 - Max 38.624 Kbps
- Receive:** Displays link speed and throughput data:
 - Link Speed >> 54.0 Mbps
 - Throughput >> 81.608 Kbps
 - Max 146.840 Kbps
- HT:** Displays bandwidth, GI, MCS, SNR0, and SNR1 settings:
 - BW >> 40
 - GI >> long
 - MCS >> 15
 - SNR0 >> 19
 - SNR1 >> n/a

PIN Method: Configure AP as Enrollee

1. In the WPS configuration page, change the Role to Enrollee. Then press Start.
2. Jot down the WPS PIN (eg. 25879810).

Configuration

▼ WPS

Parameters

WPS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Role	<input type="radio"/> Registrar <input checked="" type="radio"/> Enrollee
WPS PIN	25879810
Mode	PIN

Start **Cancel**

3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code column then choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PIN button to run the scan.

Profile Network Advanced Statistics WMM WPS Radio On/Off About

WPS AP List

ID : 0x0000	wlan-ap	00-1D-92-C0-13-CD	1
ID :	D2-VPN	00-1B-11-E4-DA-D5	7

WPS Profile List

ExRegNWEA4036

Rescan Information Pin Code 25879810 Renew

Config Mode Registrar Detail Connect Rotate Disconnect Export Profile

Status >> Disconnected

Extra Info >>

Channel >>

Authentication >>

Encryption >>

Network Type >>

IP Address >>

Sub Mask >>

Default Gateway >>

Link Quality >> 0%

Signal Strength 1 >> 0%

Signal Strength 2 >> 0%

Noise Strength >> 0%

Transmit

Link Speed >> Max

Throughput >> 0.000 Kbps

Receive

Link Speed >> Max

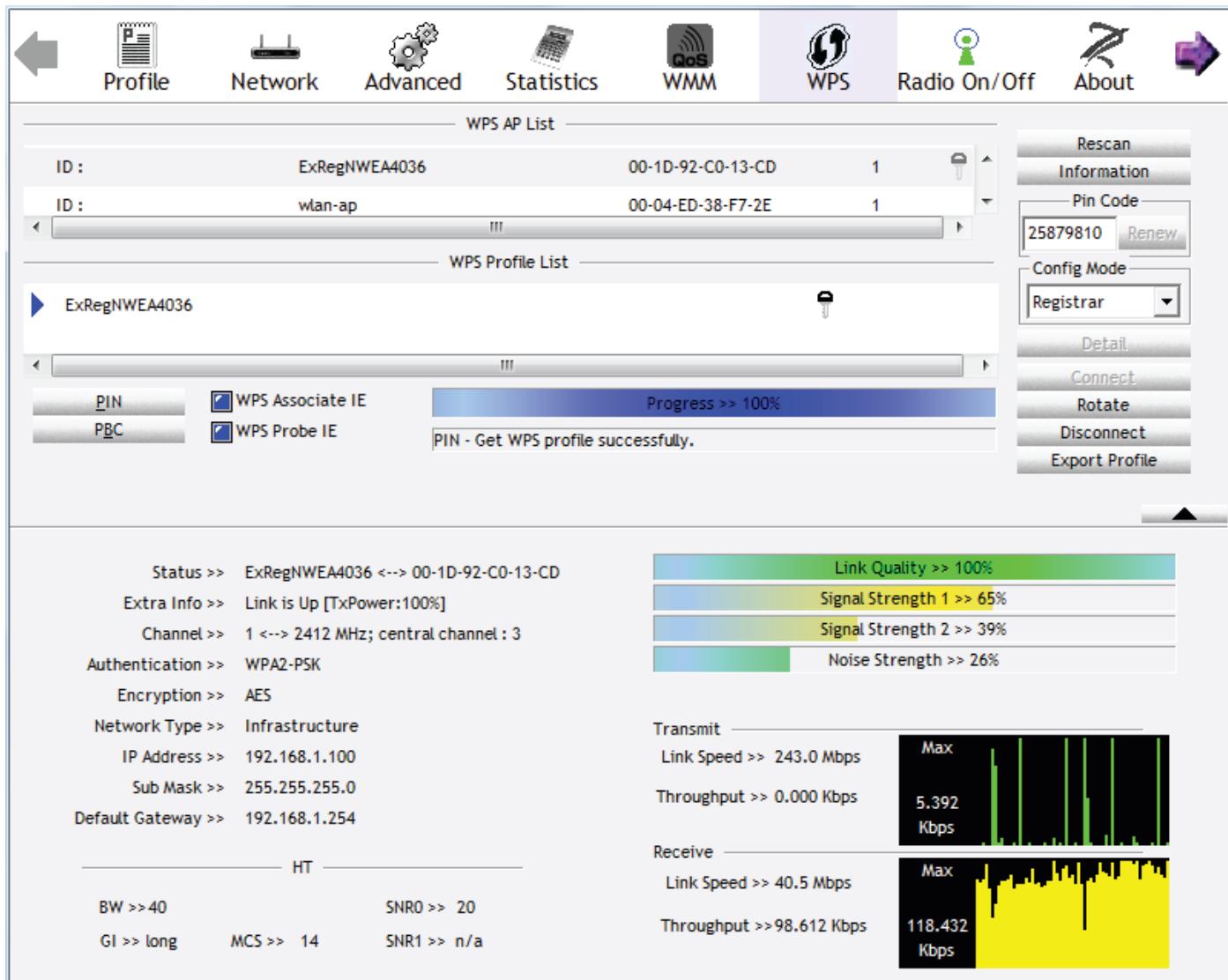
Throughput >> 0.000 Kbps

HT

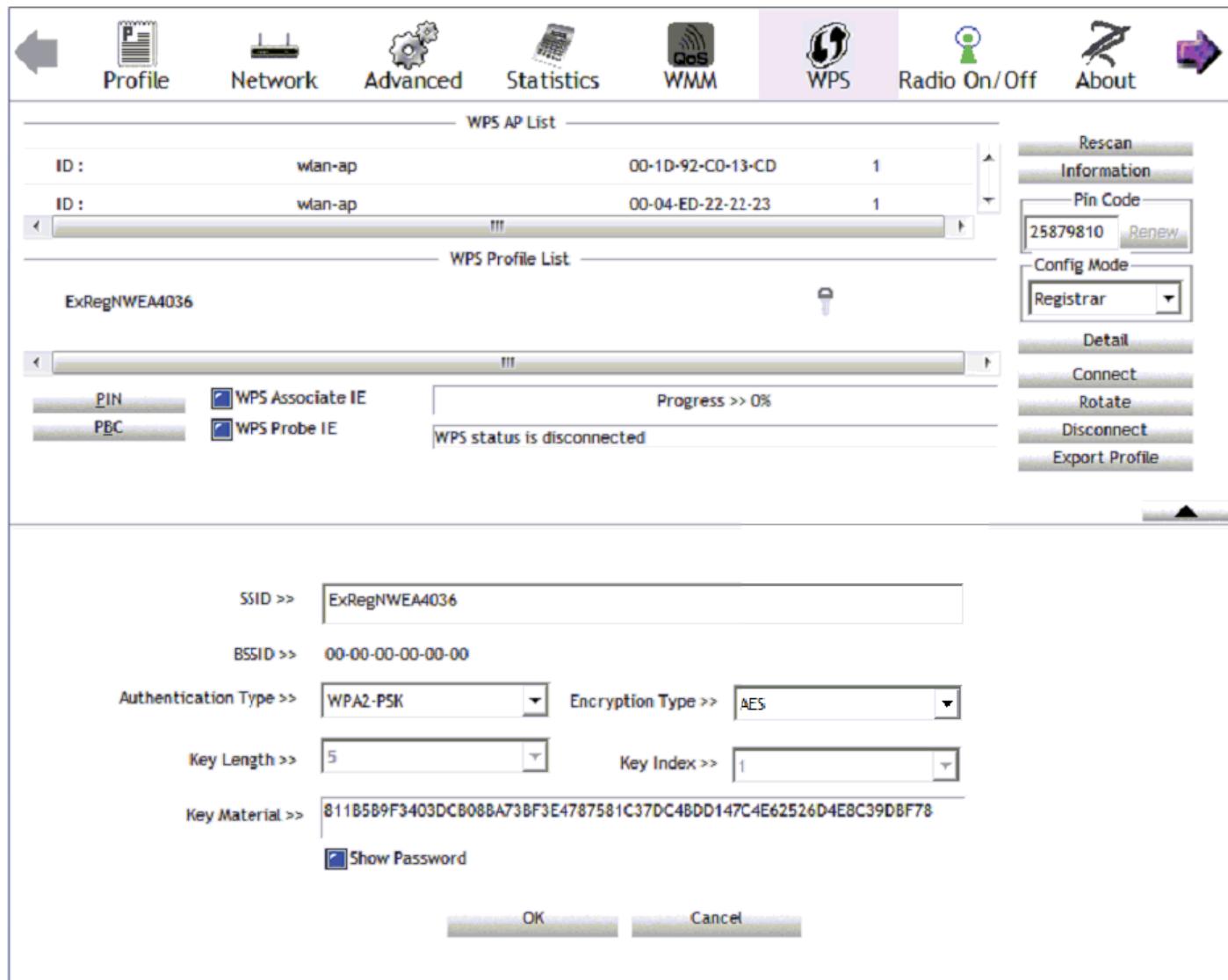
BW >> n/a SNR0 >> n/a

GI >> n/a MCS >> n/a SNR1 >> n/a

4. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar.



5. Now to make sure that the setup is correctly done, cross check to see if the SSID and the security setting of the registrar setting match with the parameters found on both Wireless Configuration and Wireless Security Configuration page.



The parameters on both Wireless Configuration and Wireless Security Configuration page are as follows:

Configuration

Wireless

Parameters

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time Schedule	1. Always On <input type="button" value="▼"/> 2. TimeSlot1 <input type="button" value="▼"/>
Mode	802.11b + g <input type="button" value="▼"/>
ESSID	wlan-ap
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Regulation Domain	N.America <input type="button" value="▼"/>
Channel ID	Channel 1 (2.412 GHz) <input type="button" value="▼"/>
Tx Power Level	100 (0 ~ 100)
AP MAC Address	00:1D:92:C0:13:CD
AP Firmware Version	RT2561T 1.1.3.0
WPS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WPS State	<input type="radio"/> Configured <input checked="" type="radio"/> Unconfigured
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Wireless Distribution System (WDS)	
WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Peer WDS MAC address	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>

Apply **Cancel** **Security settings ▶**

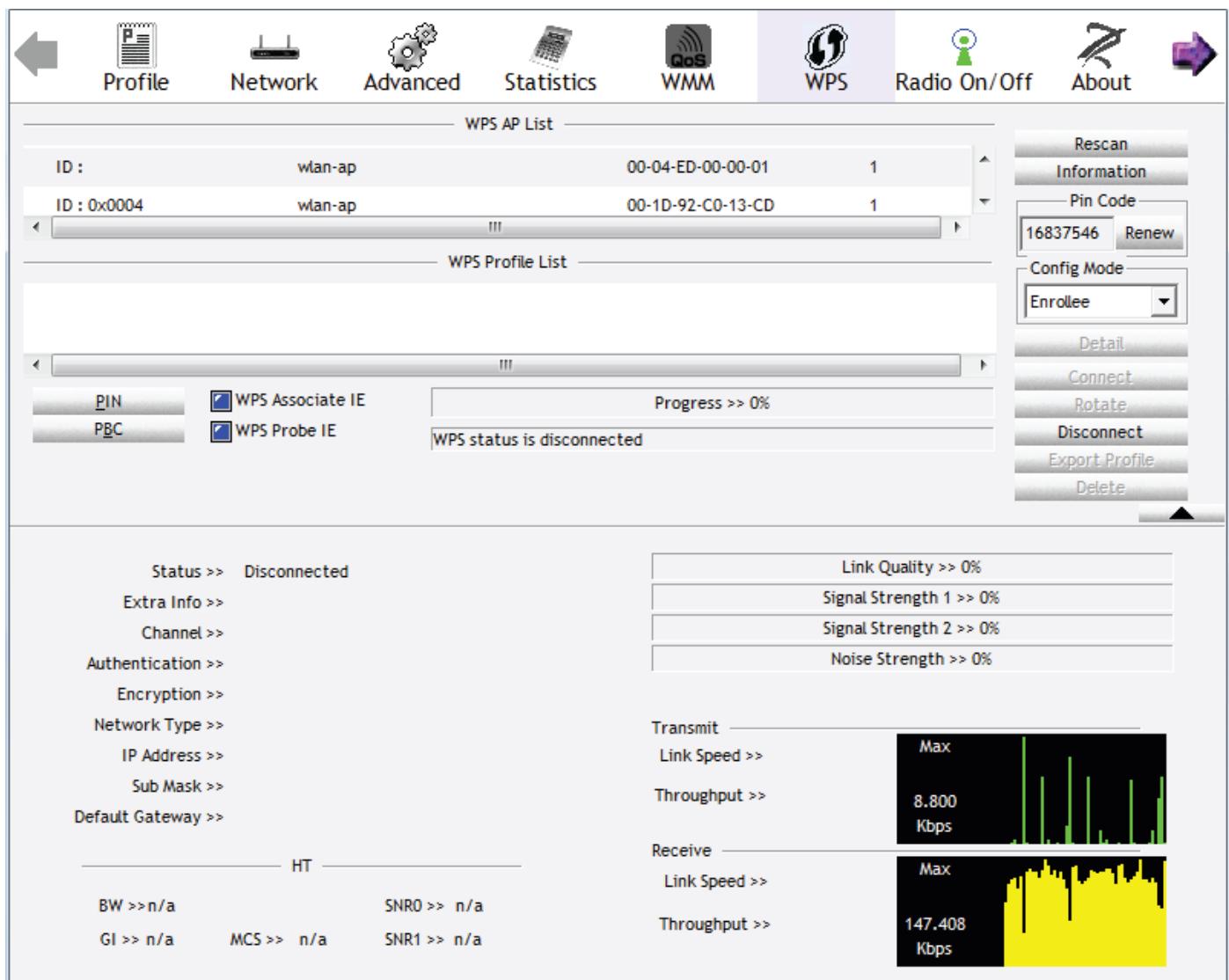
Configuration

Wireless Security

Parameters	
Security Mode	WPAWPA2-PSK
WPA Algorithms	AES
WPA Shared Key	811B5B9F3403DCB08
Group Key Renewal	3600 seconds

PBC Method:

1. Press the PBC button of the AP.
2. Launch the wireless client's WPS Utility (eg. Ralink Utility). Set the Config Mode as Enrollee. Then press the WPS button and choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PBC button to run the scan.



3. When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.

The screenshot shows a software interface for managing a wireless network. The top navigation bar includes icons for Profile, Network, Advanced, Statistics, WMM, WPS (selected), Radio On/Off, and About. The WPS AP List section shows two entries: 'wlan-ap' with MAC address 00-1D-92-C0-13-CD and 'wlan-ap' with MAC address 00-04-ED-38-F7-2E. The WPS Profile List section shows a single profile named 'wlan-ap'. On the right, a sidebar provides options for Rescan, Information, Pin Code (16837546, Renew), Config Mode (Enrollee), and various actions (Detail, Connect, Rotate, Disconnect, Export Profile, Delete). Below the profiles, a status summary and a noise strength graph are displayed. The status summary includes: Status >> wlan-ap <-> 00-1D-92-C0-13-CD, Extra Info >> Link is Up [TxPower:100%], Channel >> 1 <-> 2412 MHz; central channel : 3, Authentication >> Open, Encryption >> NONE, Network Type >> Infrastructure, IP Address >> 192.168.1.100, Sub Mask >> 255.255.255.0, and Default Gateway >> 192.168.1.254. The noise strength graph shows Link Quality >> 100%, Signal Strength 1 >> 60%, Signal Strength 2 >> 44%, and Noise Strength >> 26%. The bottom section shows HT parameters: BW >> 40, GI >> long, SNR0 >> 20, MCS >> 14, SNR1 >> n/a, and a transmit/receive throughput graph.

WPS AP List

ID :	wlan-ap	00-1D-92-C0-13-CD	1
ID :	wlan-ap	00-04-ED-38-F7-2E	1

WPS Profile List

wlan-ap

WPS Status

- PIN
- WPS Associate IE
- WPS Probe IE

Progress >> 100%

PBC - Get WPS profile successfully.

Link Status

- Status >> wlan-ap <-> 00-1D-92-C0-13-CD
- Extra Info >> Link is Up [TxPower:100%]
- Channel >> 1 <-> 2412 MHz; central channel : 3
- Authentication >> Open
- Encryption >> NONE
- Network Type >> Infrastructure
- IP Address >> 192.168.1.100
- Sub Mask >> 255.255.255.0
- Default Gateway >> 192.168.1.254

Link Quality

Link Quality >> 100%
Signal Strength 1 >> 60%
Signal Strength 2 >> 44%
Noise Strength >> 26%

Transmit

- Link Speed >> 243.0 Mbps
- Throughput >> 0.192 Kbps

Max
37.696 Kbps

Receive

- Link Speed >> 81.0 Mbps
- Throughput >> 93.732 Kbps

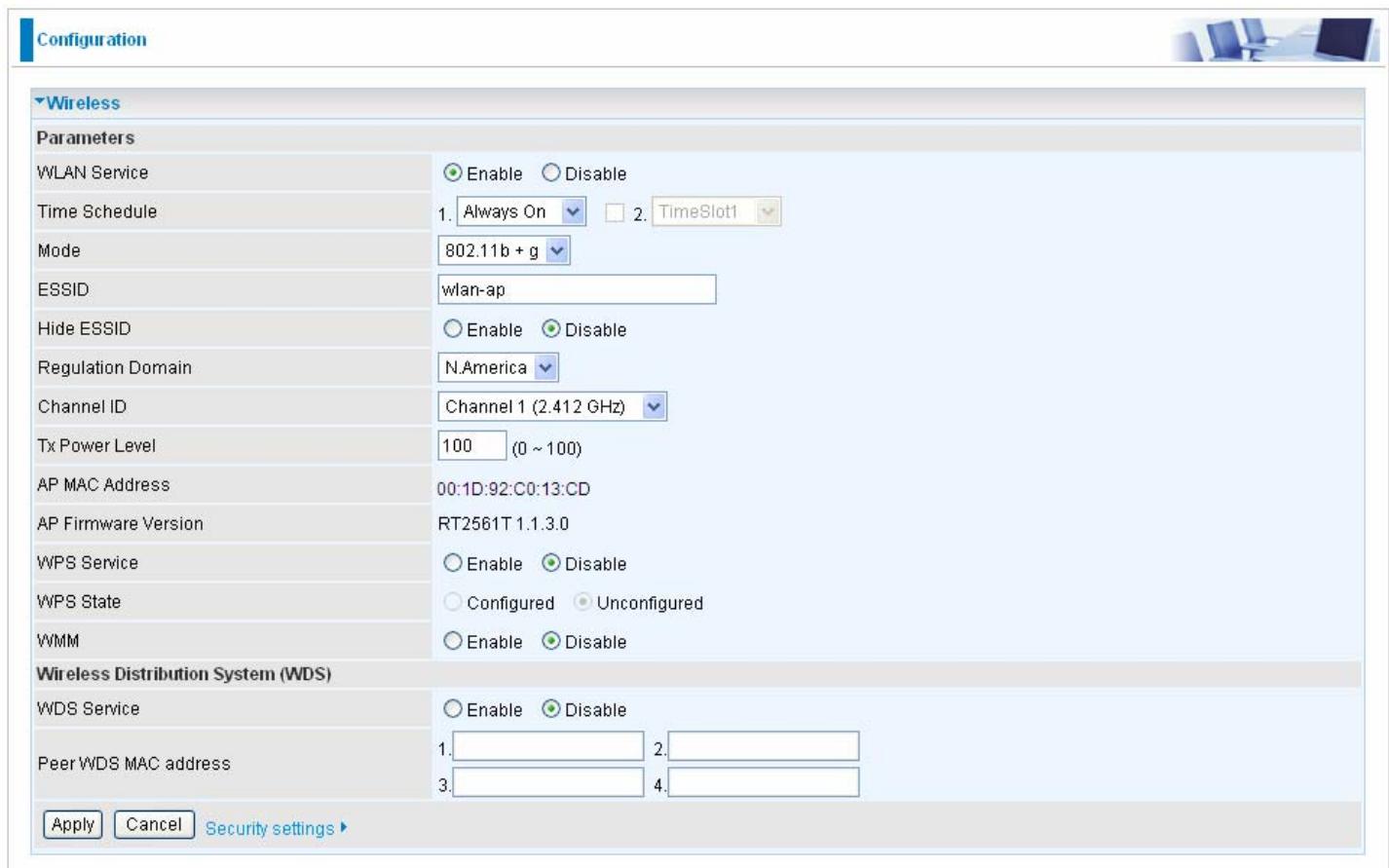
Max
1.798 Mbps

HT

BW >> 40	SNR0 >> 20	
GI >> long	MCS >> 14	SNR1 >> n/a

Wi-Fi Network Setup with Windows Vista WCN:

1. Jot down the AP PIN from the Web (eg. 25879810).
2. Access the Wireless configuration of the web GUI. Set the WPS State to Unconfigured then click Apply.



The screenshot shows the 'Configuration' window for the 'Wireless' section. The 'Parameters' tab is selected. Key settings include:

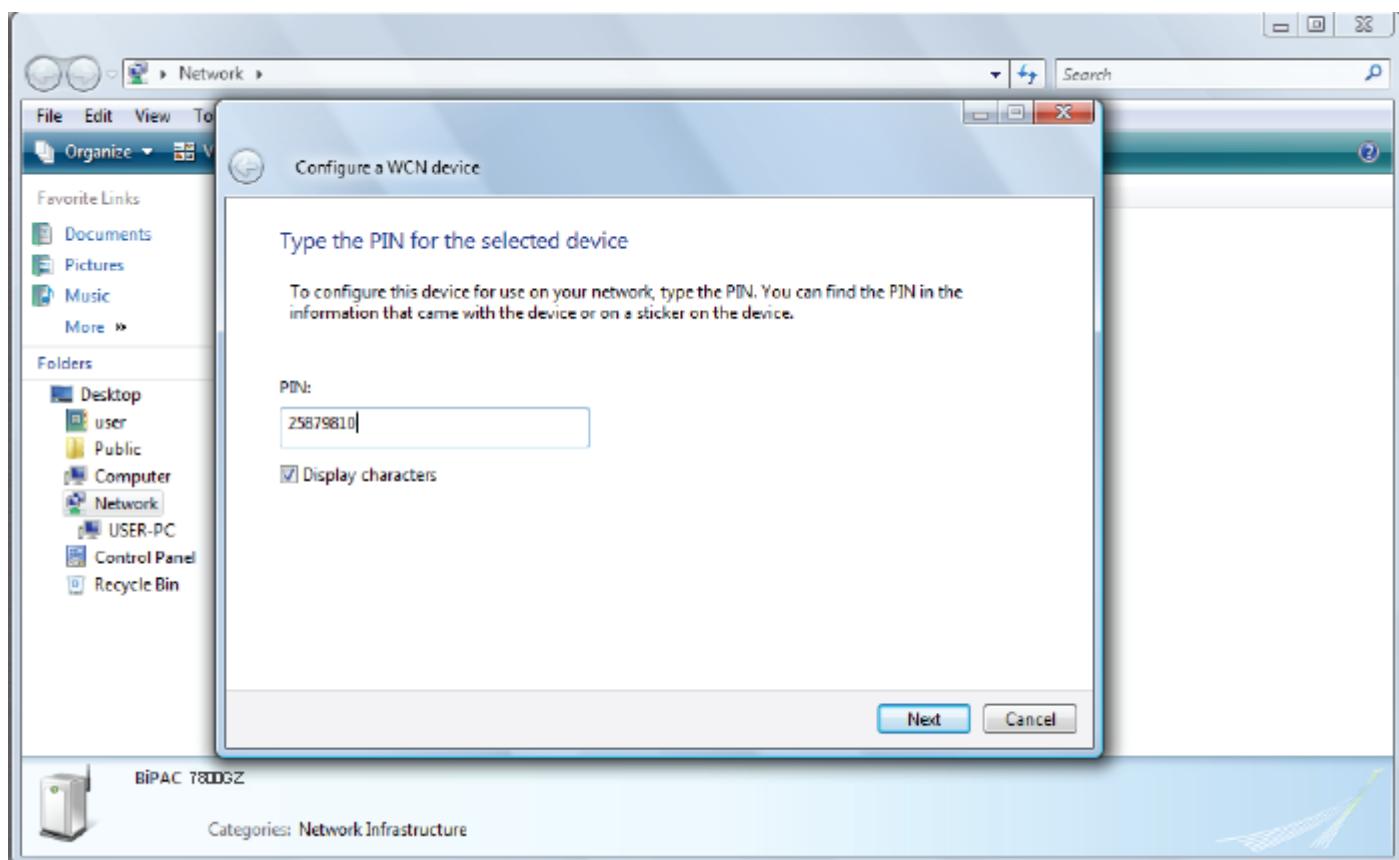
- WLAN Service: Enable (radio button selected)
- Time Schedule: 1. Always On, 2. TimeSlot1
- Mode: 802.11b + g
- ESSID: wlan-ap
- Hide ESSID: Disable (radio button selected)
- Regulation Domain: N.America
- Channel ID: Channel 1 (2.412 GHz)
- Tx Power Level: 100 (0 ~ 100)
- AP MAC Address: 00:1D:92:C0:13:CD
- AP Firmware Version: RT2561T 1.1.3.0
- WPS Service: Disable (radio button selected)
- WPS State: Unconfigured (radio button selected)
- WMM: Disable (radio button selected)

The 'Wireless Distribution System (WDS)' tab is also visible, showing:

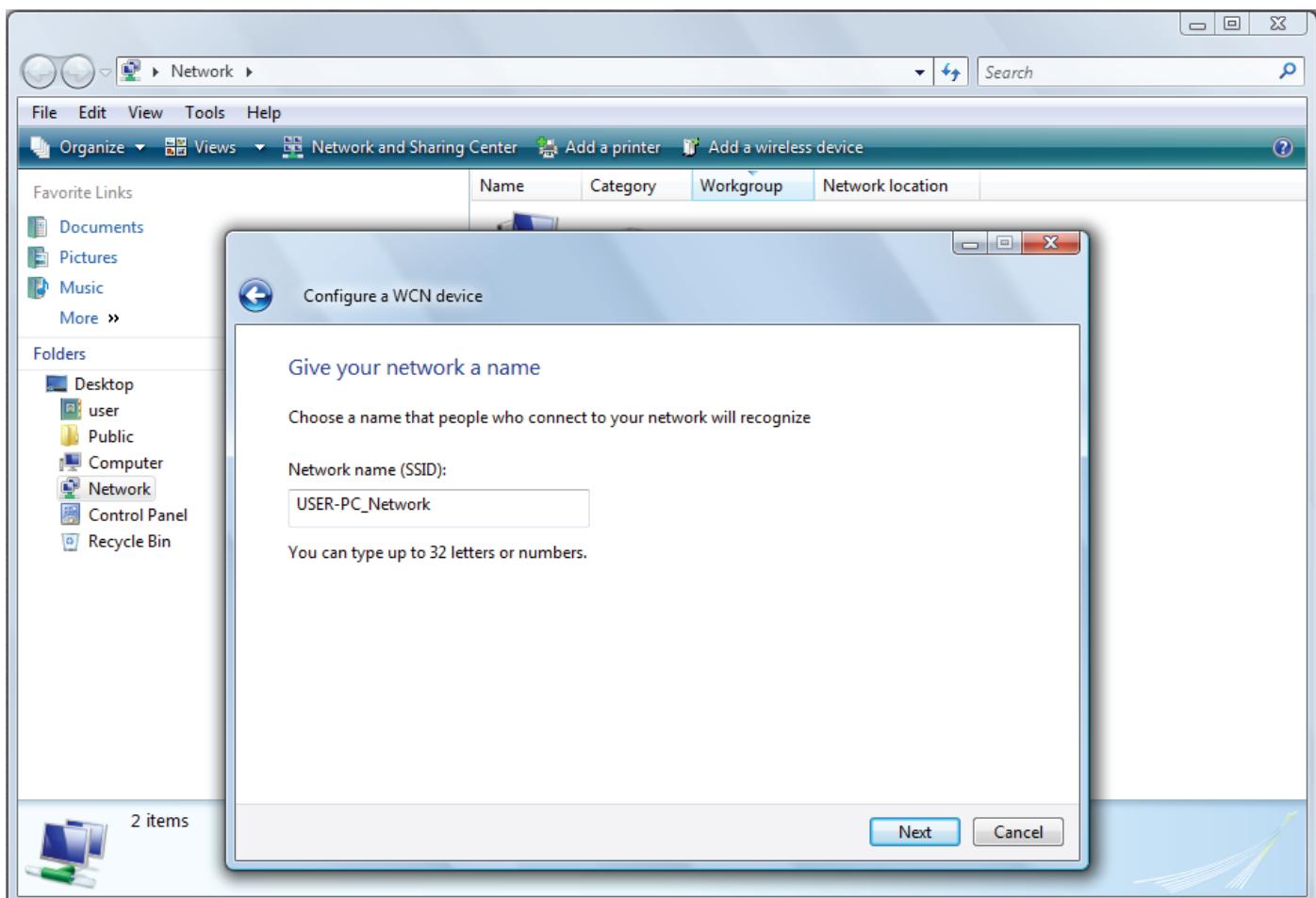
- WDS Service: Disable (radio button selected)
- Peer WDS MAC address: 1. [] 2. [] 3. [] 4. []

At the bottom are 'Apply', 'Cancel', and 'Security settings' buttons.

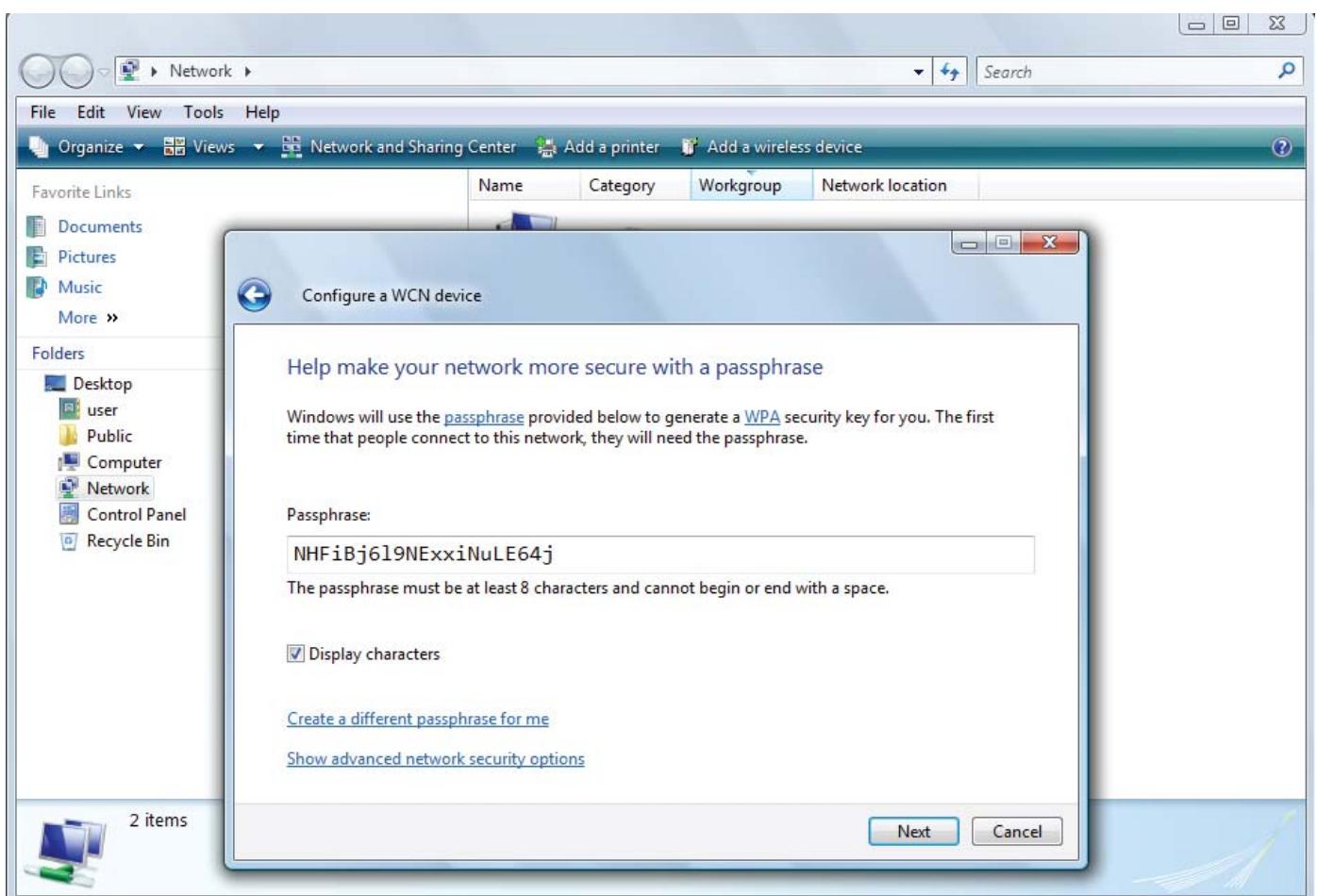
3. In your Vista operating system, access the Control Panel page, then select Network and Internet > View Network Computers and Devices. Double click on the BiPAC 7800GZ(L) icon and enter the AP PIN in the column provided then press Next.



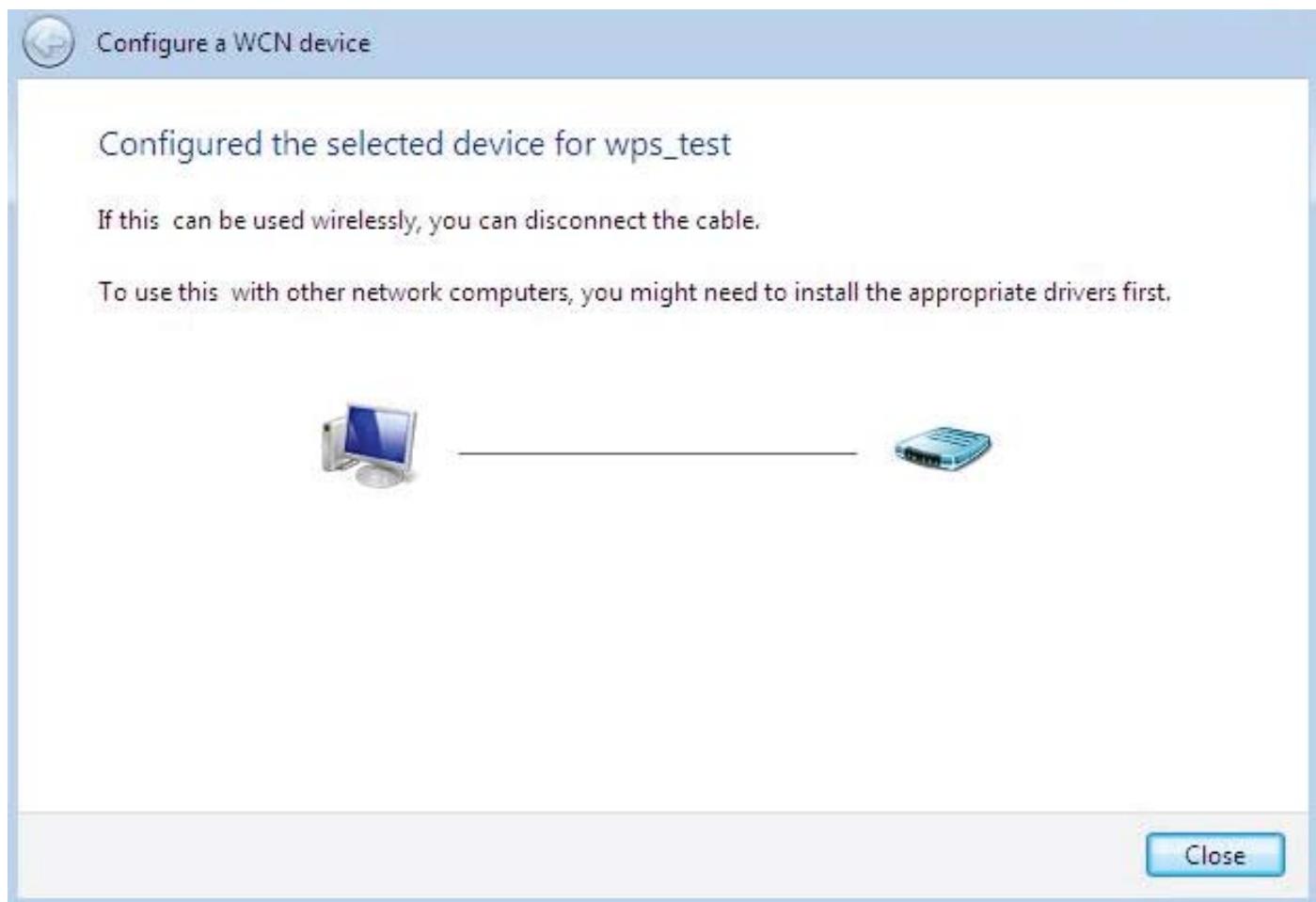
4. Enter the AP SSID then click Next.



5. Enter the Passphrase then click Next.

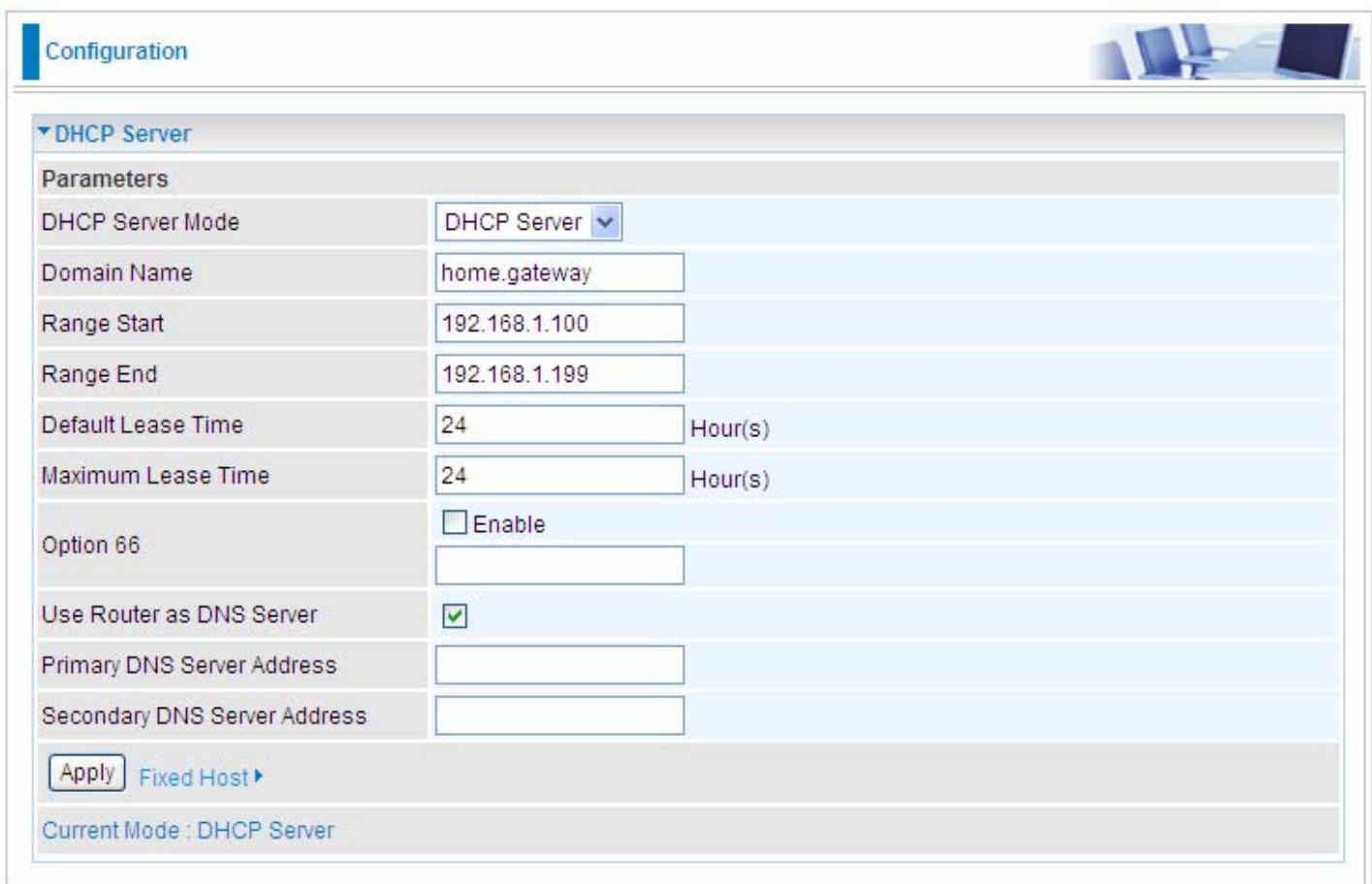


6. When you have come to this step, you will have completed the Wi-Fi network setup using the built-in WCN feature in Windows Vista.



DHCP Server

DHCP allows networked devices to obtain information on the parameter of IP, Netmask, Gateway as well as DNS through the Ethernet Address of the device.



The screenshot shows a configuration interface for a DHCP server. The 'DHCP Server Mode' is set to 'DHCP Server'. The 'Domain Name' is 'home.gateway'. The 'Range Start' is '192.168.1.100' and the 'Range End' is '192.168.1.199'. The 'Default Lease Time' and 'Maximum Lease Time' are both set to 24 hours. The 'Option 66' field is empty and has an 'Enable' checkbox. The 'Use Router as DNS Server' checkbox is checked. The 'Primary DNS Server Address' and 'Secondary DNS Server Address' fields are empty. At the bottom, there are 'Apply' and 'Fixed Host' buttons, and a note 'Current Mode : DHCP Server'.

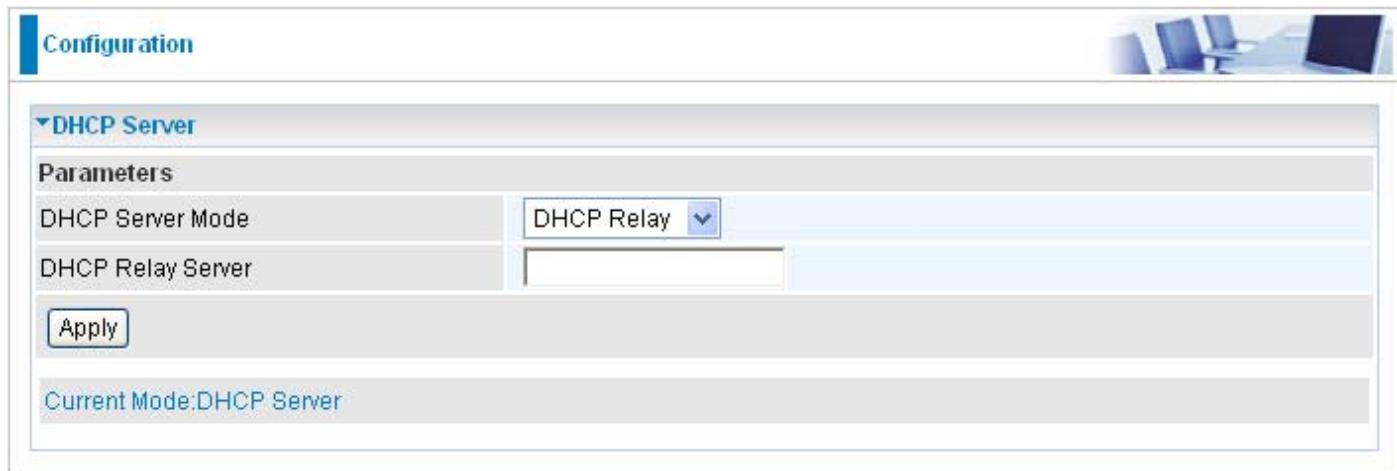
To configure the router's DHCP Server, select **DHCP Server** from the DHCP Server Mode drop-down menu. You can then configure parameters of the DHCP Server including the domain, IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. If you check "Use Router as a DNS Server", the ADSL Router will perform the domain name lookup, find the IP address from the outside network automatically and forward it back to the requesting PC in the LAN (your Local Area Network).

Note:

Option 66: This option is used to identify a TFTP server, User must set TFTP server IP address if enable option 66.

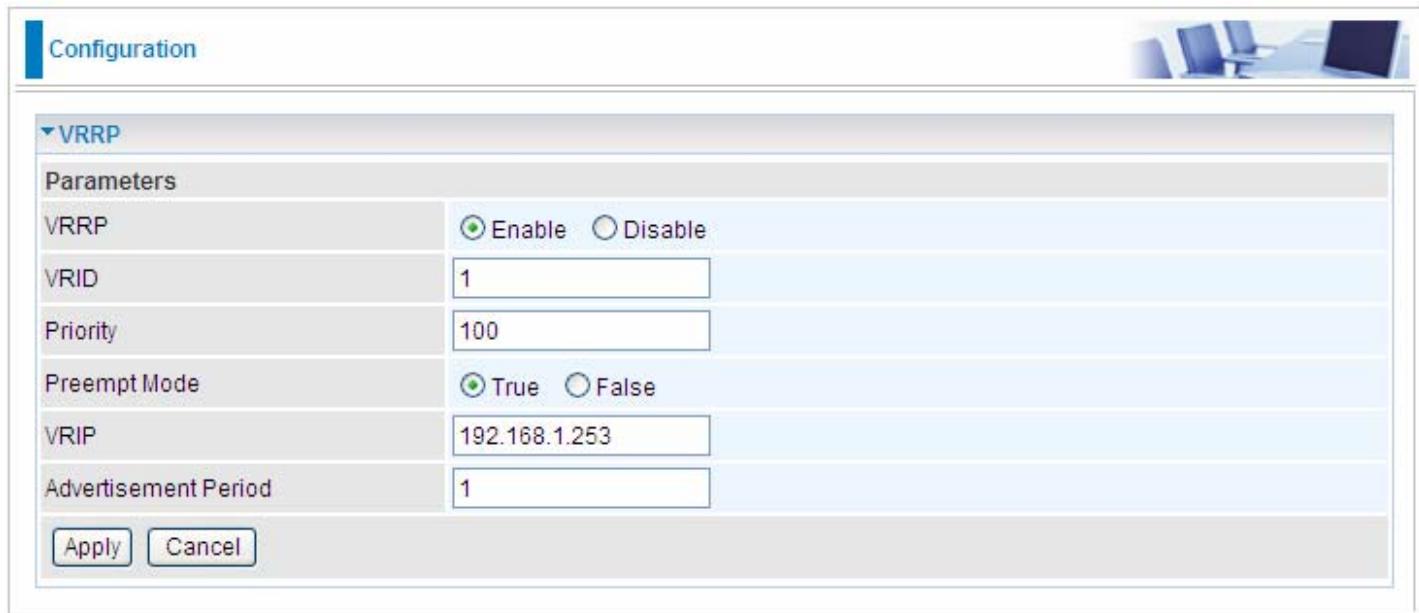
Click Apply to enable this function.

If you select **DHCP Relay** from the DHCP Server Mode drop-down menu, you must enter the IP address of the DHCP server that assigns an IP address to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP. Click Apply to enable this function.



VRP

VRP is designed to eliminate the single point of failure inherent in the static default routed environment. VRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRP routers in a LAN. The VRP router controlling the IP address associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility should the Master become unavailable. Any of the virtual router's IP addresses in a LAN can then be used as the default first hop router by end-hosts. The advantage gained from using VRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.



The screenshot shows a configuration interface for VRP. The 'Parameters' section contains the following fields:

VRP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
VRID	1
Priority	100
Preempt Mode	<input checked="" type="radio"/> True <input type="radio"/> False
VRIP	192.168.1.253
Advertisement Period	1

At the bottom are 'Apply' and 'Cancel' buttons.

VRP: The default setting is **Disable**. Check **Enable** radio button to activate this function.

VRID: A master or backup router running the VRP protocol may participate in one VRID instance.

Priority: Specifies the sending VRP router's priority for the virtual router. Higher values equal higher priority. The priority value for the VRP router that owns the IP address associated with the virtual router **MUST** be **255**. VRP routers backing up a virtual router **MUST** use priority values between **1** and **254**. The default priority value for VRP routers backing up a virtual router is **100**. The priority value zero (0) has special meaning indicating that the current Master has stopped participating in VRP. This is used to trigger Backup routers to quickly transition to Master without having to wait for the current Master to timeout.

Preempt Mode: When preempt mode is enabled, a backup router always takes over the responsibility of the master router. When disabled, the lower priority backup is left in the master state.

VRIP: One IP address that is associated with the virtual router.

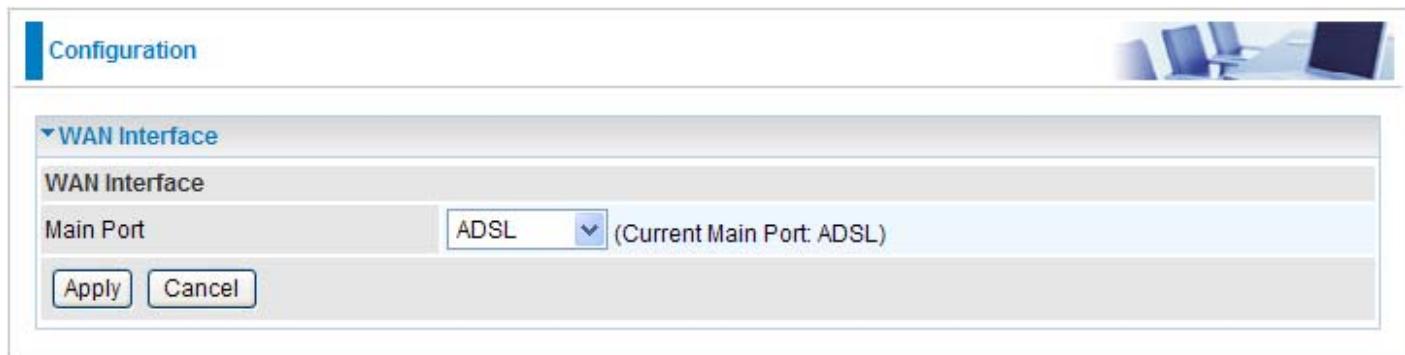
Advertisement period: Indicates the time interval in seconds between advertisements. The default value is 1 second.

WAN - Wide Area Network

A WAN (Wide Area Network) is a computer network that covers a broad geographical area (e.g. Internet) that is used to connect LAN and other types of network systems. There are 4 items within the WAN section: **WAN Interface**, **WAN Profile**, **Mobile Networks** and **ADSL Mode**.

WAN Interface

ADSL

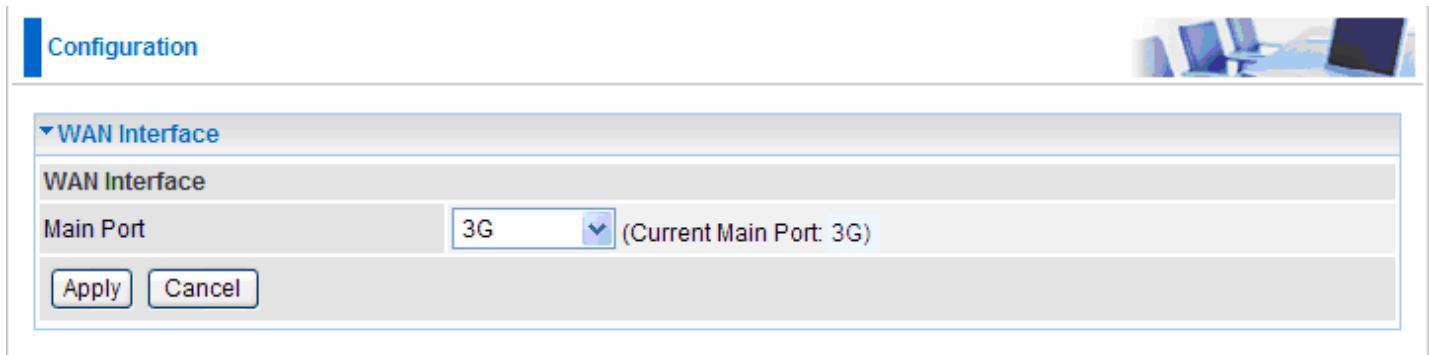


The screenshot shows a configuration interface for the WAN Interface. The main title is 'Configuration' with a 'WAN Interface' sub-section. Under 'WAN Interface', there is a 'Main Port' dropdown menu set to 'ADSL' (Current Main Port: ADSL). Below the dropdown are 'Apply' and 'Cancel' buttons. The background features a blurred image of a computer workstation.

Main Port: Select the main port from the drop-down menu.

Click Apply to confirm the change.

3G

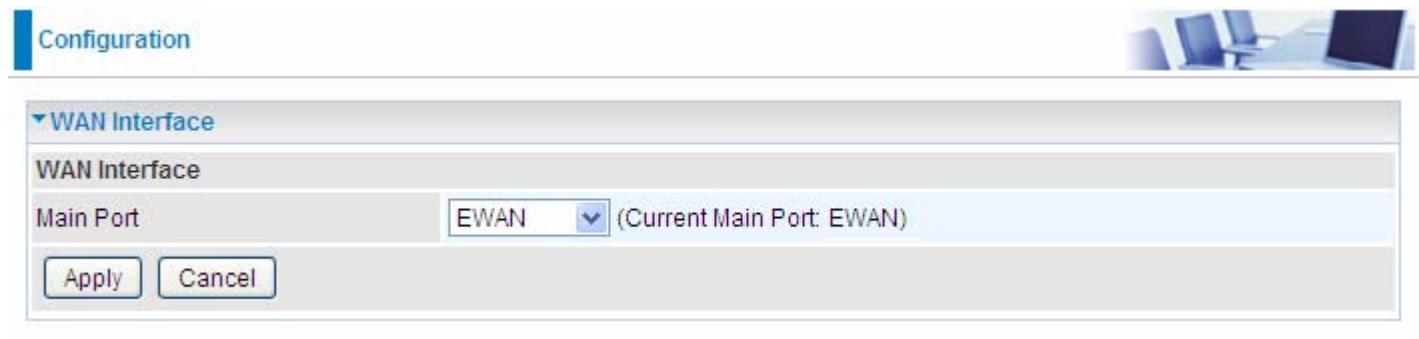


The screenshot shows a configuration interface for the WAN Interface. The main title is 'Configuration' with a 'WAN Interface' sub-section. Under 'WAN Interface', there is a 'Main Port' dropdown menu set to '3G' (Current Main Port: 3G). Below the dropdown are 'Apply' and 'Cancel' buttons. The background features a blurred image of a computer workstation.

Main Port: Select the main port from the drop-down menu.

Click Apply to confirm the change.

EWAN

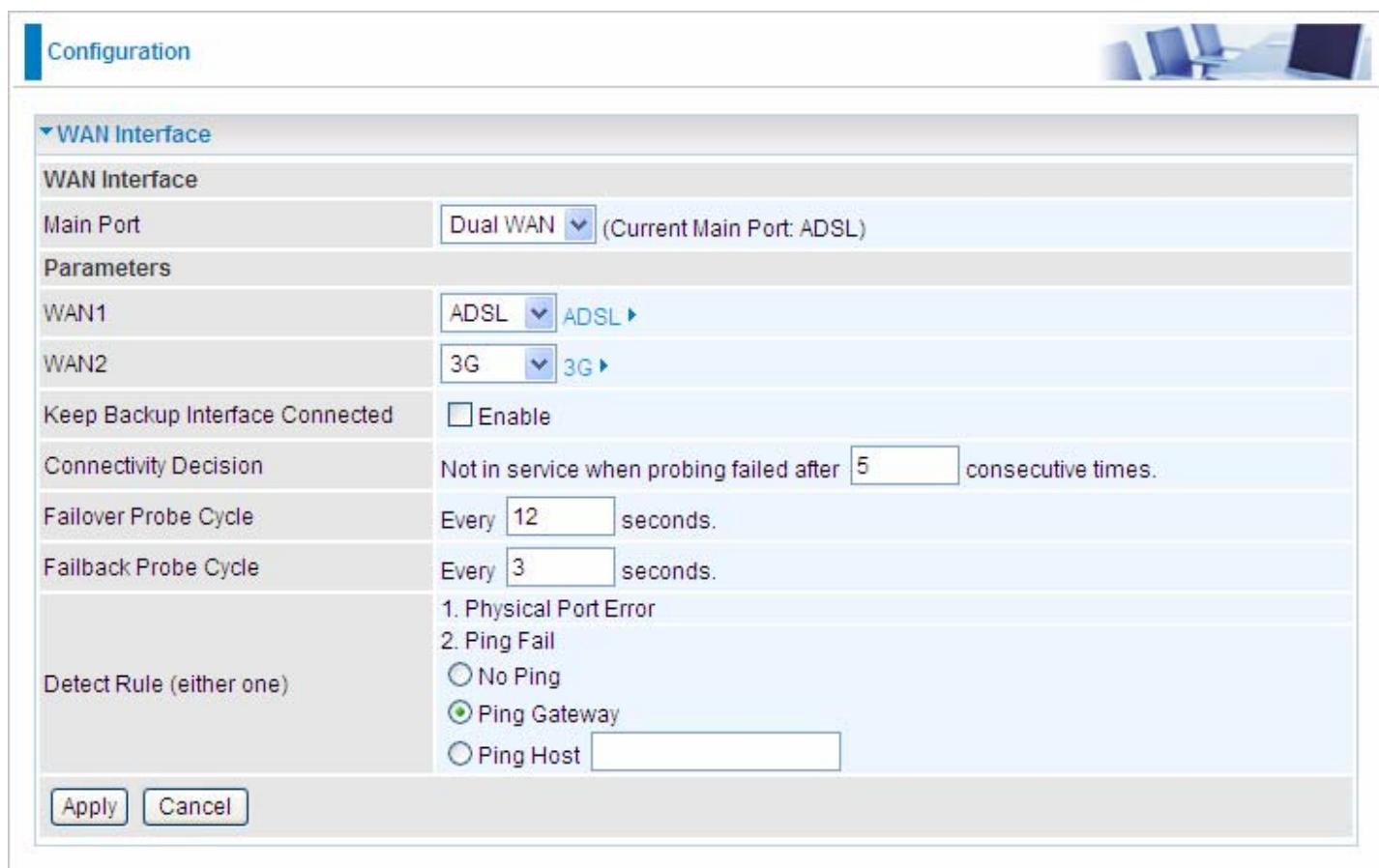


The screenshot shows the 'Configuration' tab selected in the top navigation bar. Under the 'WAN Interface' section, the 'Main Port' dropdown is set to 'EWAN' (Current Main Port: EWAN). Below the dropdown are 'Apply' and 'Cancel' buttons.

Main Port: Select the main port from the drop-down menu.

Click Apply to confirm the change.

Dual WAN



The screenshot shows the 'Configuration' tab selected in the top navigation bar. Under the 'WAN Interface' section, the 'Main Port' dropdown is set to 'Dual WAN' (Current Main Port: ADSL). The 'Parameters' section includes settings for 'WAN1' (ADSL), 'WAN2' (3G), 'Keep Backup Interface Connected' (Enable), 'Connectivity Decision' (Not in service when probing failed after 5 consecutive times), 'Failover Probe Cycle' (Every 12 seconds), 'Fallback Probe Cycle' (Every 3 seconds), and a 'Detect Rule' section with options for Physical Port Error, Ping Fail, and Ping Host. Below the parameters are 'Apply' and 'Cancel' buttons.

Main Port: Select the main port from the drop-down menu.

WAN1: Choose ADSL EWAN or 3G for WAN1. Click the link to go to WAN Profile page to configure its parameters.

WAN2: Choose ADSL EWAN or 3G for WAN2. Click the link to go to WAN Profile page to configure its parameters.

Keep Backup Interface Connected: Select Enable this function, the backup port WAN2 will be connected all the time.

Connectivity Decision: Enter the value for the times when probing failed to switch backup port.

Failover Probe Cycle: Set the time duration for the Failover Probe Cycle to determine when the router will switch to the backup connection (backup port) once the main connection (main port) fails.

Failback Probe Cycle: Set the time duration for the Failback Probe Cycle to determine when the router will switch back to the main connection (main port) from the backup connection (backup port) once the main connection communicates again.

Note: *The time values entered in Failover Probe Cycle and Failback Probe Cycle fields are set for each probe cycle and decided by Probe Cycle duration multiplied by Connection Decision value (e.g. 60 seconds are multiplied by 12 seconds and 5 consecutive fails).*

Detect Rule (either one):

1. **Physical Port Error**

2. **Ping Fail**

- **No Ping:** It will not send any ping packet to determine the connection. It means to disable the ping fail detection.

- **Ping Gateway:** It will send ping packet to gateway and wait response from gateway in every “Probe Cycle”.

- **Ping Host:** It will send ping packet to specific host and wait response in every “Probe Cycle”. The host must be an IP address.

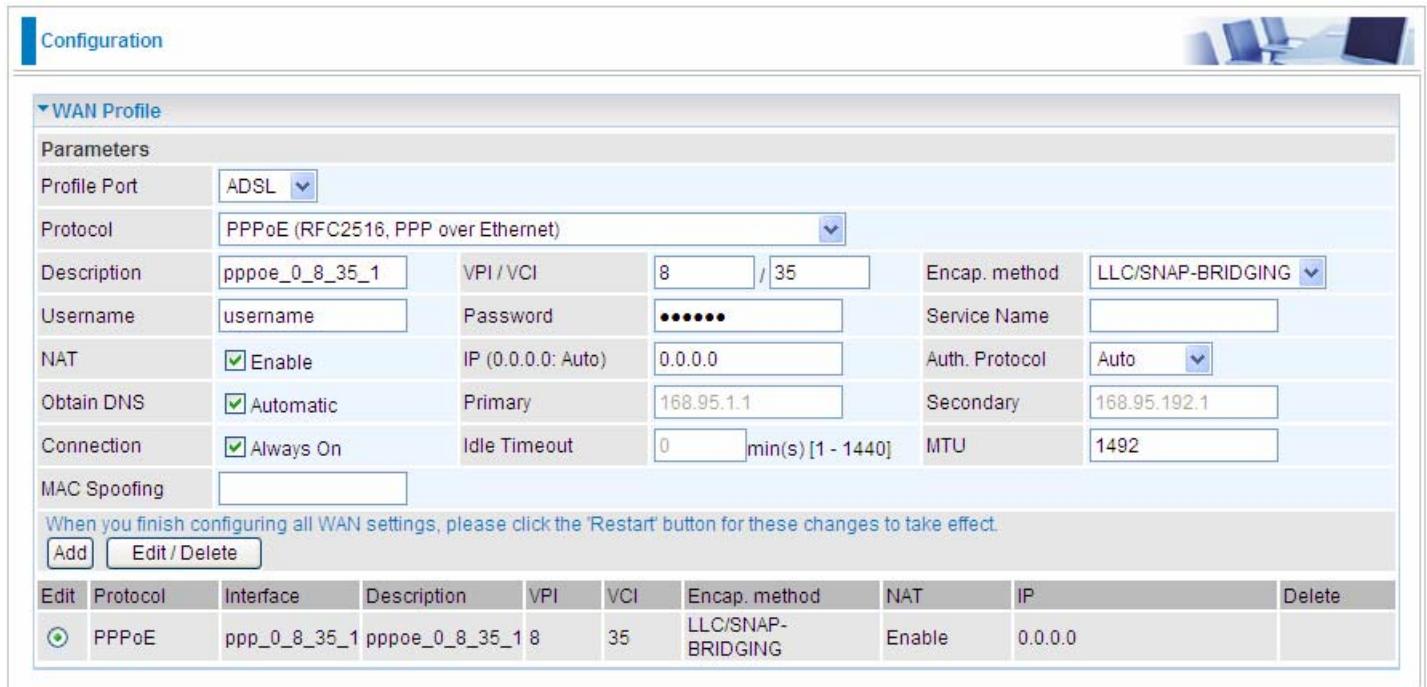
Click Apply to confirm the change.

WAN Profile

ADSL

PPPoE (ADSL)

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.



The screenshot shows the 'WAN Profile' configuration page for PPPoE (ADSL). The 'Profile Port' is set to 'ADSL'. The 'Protocol' is 'PPPoE (RFC2516, PPP over Ethernet)'. The 'Description' is 'pppoe_0_8_35_1'. The 'Username' is 'username' and the 'Password' is masked. 'NAT' is enabled. 'Obtain DNS' is automatic, with 'Primary' set to '168.95.1.1' and 'Secondary' set to '168.95.192.1'. 'Connection' is 'Always On' with an 'Idle Timeout' of 0. The 'Encap. method' is 'LLC/SNAP-BRIDGING'. The 'Service Name' and 'Auth. Protocol' are empty. The 'MTU' is 1492. The 'MAC Spoofing' field is empty. A note at the bottom says 'When you finish configuring all WAN settings, please click the 'Restart' button for these changes to take effect.' There are 'Add' and 'Edit / Delete' buttons. A table at the bottom lists the configuration with a single row: **Protocol**: PPPoE, **Interface**: ppp_0_8_35_1, **Description**: pppoe_0_8_35_1, **VPI**: 8, **VCI**: 35, **Encap. method**: LLC/SNAP-BRIDGING, **NAT**: Enable, **IP**: 0.0.0.0.

Description: A given name for the connection.

VPI/VCI: Enter the information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing a single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

IP (0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS / Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the Netmask.

Connection: Click on **Always on** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

MTU: Control the maximum Ethernet packet size your PC will send.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

PPPoA (ADSL)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functions in a manner similar to dial-up services using PPP.

Description: A given name for the connection.

VPI/VCI: Enter the information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing a single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

IP (0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

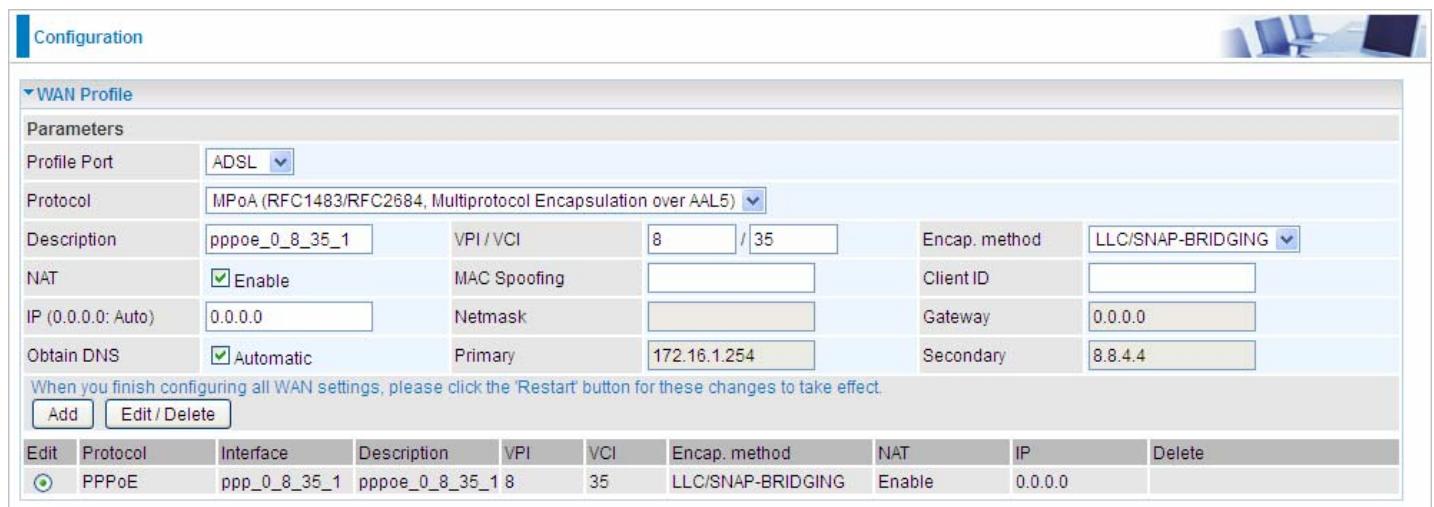
Primary DNS / Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the Netmask.

Connection: Click on **Always on** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

MTU: Control the maximum Ethernet packet size your PC will send.

MPoA (ADSL)



Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
<input checked="" type="radio"/>	PPPoE	ppp_0_8_35_1	pppoe_0_8_35_1	8	35	LLC/SNAP-BRIDGING	Enable	0.0.0.0	

Description: A given name for the connection.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account by sharing a single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

Client ID: DHCP Option 61 (Client Identifier), it is used to bind some specific DHCP assigned IP to the Client so that the client can obtain a fixed IP (the client can be an interface). Here user can get the information from your ISP.

IP (0.0.0.0:Auto): Your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both Netmask and gateway can be left blank.

Netmask: User can change it to other such as 255.255.255.128. Type the Netmask assigned to you by your ISP (if given)

Gateway: Enter the IP address of the default gateway.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS / Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the Netmask.

IPoA (ADSL)

Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
PPPoE	ppp_0_8_35_1	pppoe_0_8_35_1	8	35	LLC/SNAP-BRIDGING	Enable	0.0.0.0	

Description: A given name for the connection.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account by sharing a single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

IP Address: Enter your fixed IP address.

Netmask: User can change it to other such as 255.255.255.128. Type the Netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Obtain DNS Automatically: Select this check box to activate DNS.

Primary DNS / Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the Netmask.

Pure Bridge (ADSL)

Description: A given name for the connection.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Usage Allowance: to control 3G flow, click it to further configure about 3G flow, refer to the following [3G Usage Allowance](#) for more information.

Mode: There are 5 options of phone service standards: GSM 2G only, UMTS 3G only, GSM 2G preferred, UMTS 3G preferred, and Automatic. If you are uncertain what services are available to you, then please select Automatic.

TEL No.: The dial string to make a GPRS / 3G user internetworking call. It may provide by your mobile service provider.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. some 3G operators use the APN 'internet' for their portal. The default value is "internet".

Username/Password: Enter the username and password provided by your service provider. The username and password are case sensitive.

Authentication Protocol: Default is Auto. Please consult your service provider on whether to use PAP, CHAP or MSCHAP.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/service provider.

Connection:

Connection	<input checked="" type="radio"/> Always On <input type="radio"/> Connect on Demand
Keep Alive	<input checked="" type="checkbox"/> Enable <input type="text" value="60"/> seconds

Always On: The router will make UMTS/GPRS call when starting up. Click on Always On, the Keep Alive field will display.

Keep Alive: Check Enable to allow the router automatically send message out periodically to prevent the connection being dropped out by your ISP. Type the circle time, default is 60 seconds.

Connection	<input type="radio"/> Always On <input checked="" type="radio"/> Connect on Demand
Idle Timeout	<input type="text" value="600"/> seconds

Connect on Demand: If you want to make UMTS/GPRS call only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time. Click on Connect on Demand, the Idle Timeout field will display.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. The idle timeout value is not allowed to be set under 10 seconds. Default is 600 seconds.

NAT: Check to enable the NAT function.

Obtain DNS Automatically: Select this check box to activate DNS automatically.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the Netmask.

MTU: MTU (Maximum Transmission Unit) is the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Click Apply to confirm the settings.

Note: *If you don't know how to set these parameters, please keep them untouched.*

3G Usage Allowance

Configuration	
3G Usage Allowance	
Parameters	
Mode	<input checked="" type="radio"/> Volume-based <input type="radio"/> Time-based
Only Download	<input type="text" value="1"/> MB data volume per month included
1	hours per month included
The billing period begins on	day <input type="text" value="1"/> of a month.
Over usage allowance action	<input type="radio"/> E-mail Alert
E-mail alert at percentage of bandwidth	<input type="text" value="80"/> %
Save the statistics to ROM	<input type="radio"/> Every one hours
Buttons	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Return ▶"/>	

Mode: include **Volume-based** and **Time-based** control.

Volume-based include “only Download”, “only Upload” and “Download and Upload” to limit the flow.

Time-based control the flow by providing specific hours per month.

The billing period begins on: the beginning day of billing each month.

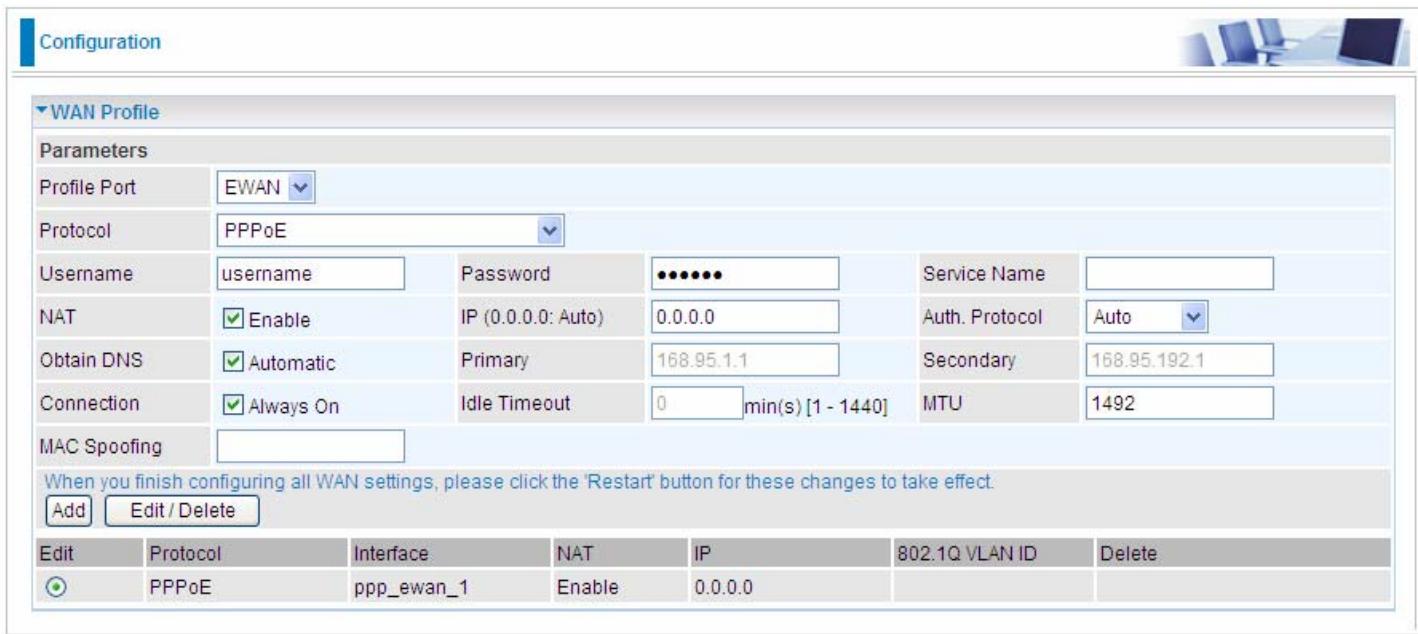
Over usage allowance action: what to do when the flow is over usage allowance, the available methods are “E-mail Alert”, “Email Alert and Disconnect” and “Disconnect”.

E-mail alert at percentage of bandwidth: When the used bandwidth exceeds the set proportion, the system will send email to alert.

Save the statistics to ROM: to save the statistics to ROM system.

EWAN

PPPoE (EWAN)



The screenshot shows the 'WAN Profile' configuration for the 'EWAN' port. The 'Protocol' is set to 'PPPoE'. The 'Username' is 'username' and the 'Password' is '*****'. The 'Service Name' is empty. Under 'NAT', 'Enable' is checked and 'IP (0.0.0.0: Auto)' is set to '0.0.0.0'. The 'Auth. Protocol' is 'Auto'. Under 'Obtain DNS', 'Automatic' is checked, with 'Primary' set to '168.95.1.1' and 'Secondary' set to '168.95.192.1'. Under 'Connection', 'Always On' is checked, and 'Idle Timeout' is set to '0 min(s) [1 - 1440]'. The 'MTU' is '1492'. The 'MAC Spoofing' field is empty. A note at the bottom says: 'When you finish configuring all WAN settings, please click the 'Restart' button for these changes to take effect.' Below the configuration table is a smaller table showing the current WAN settings:

Edit	Protocol	Interface	NAT	IP	802.1Q VLAN ID	Delete
<input checked="" type="radio"/>	PPPoE	ppp_ewan_1	Enable	0.0.0.0		

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing a single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

IP (0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS / Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

Connection: Click on **Always on** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

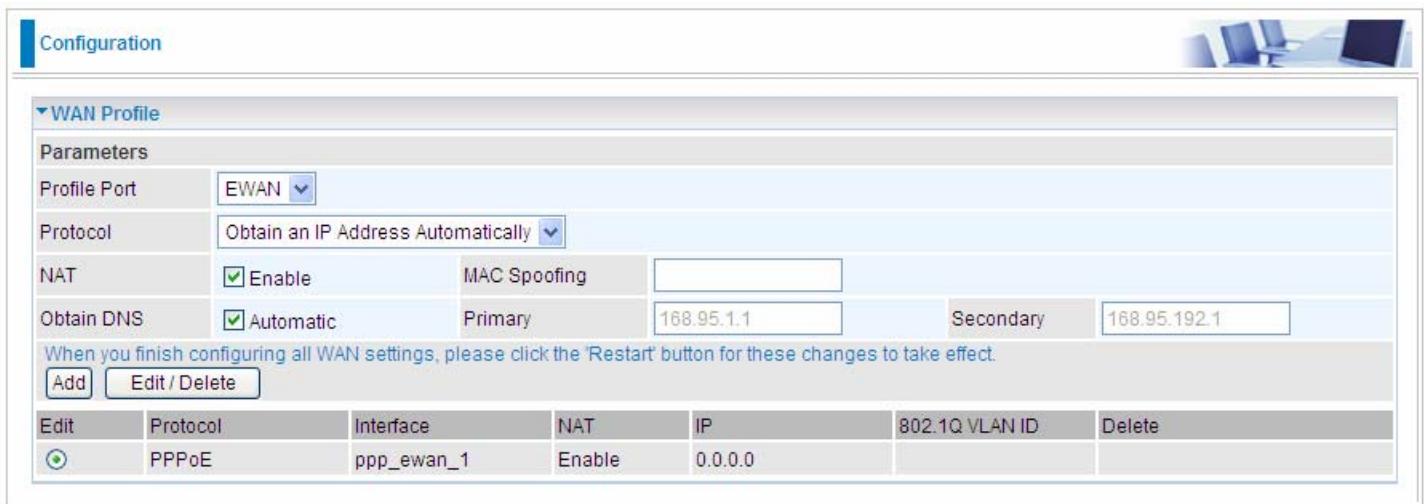
MTU: Control the maximum Ethernet packet size your PC will send.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address

specified by your service provider when this information is required. The default setting is set to disable.

Click Apply to confirm the settings.

Obtain an IP Address Automatically (EWAN)



The screenshot shows the 'Configuration' interface with the 'WAN Profile' section selected. The 'Profile Port' is set to 'EWAN'. The 'Protocol' is set to 'Obtain an IP Address Automatically'. Under 'NAT', 'Enable' is checked. Under 'Obtain DNS', 'Automatic' is checked, with 'Primary' set to '168.95.1.1' and 'Secondary' set to '168.95.192.1'. A note at the bottom says 'When you finish configuring all WAN settings, please click the 'Restart' button for these changes to take effect.' Below this are 'Add', 'Edit / Delete' buttons, and a table for protocols:

Edit	Protocol	Interface	NAT	IP	802.1Q VLAN ID	Delete
<input checked="" type="radio"/>	PPPoE	ppp_ewan_1	Enable	0.0.0.0		

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

Obtain DNS: Select this check box to activate DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the Netmask.

Click Apply to confirm the settings.

Fixed IP Address (EWAN)

Configuration

WAN Profile

Parameters

Profile Port	EWAN		
Protocol	Fixed IP Address		
NAT	<input checked="" type="checkbox"/> Enable	MAC Spoofing	
IP Address		Netmask	
Obtain DNS	<input type="checkbox"/> Automatic	Primary	168.95.1.1
		Secondary	168.95.192.1

When you finish configuring all WAN settings, please click the 'Restart' button for these changes to take effect.

Add Edit / Delete

Edit	Protocol	Interface	NAT	IP	802.1Q VLAN ID	Delete
<input checked="" type="radio"/>	PPPoE	ppp_ewan_1	Enable	0.0.0.0		

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

MAC Spoofing: This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

IP Address: Enter your fixed IP address.

Netmask: User can change it to others such as 255.255.255.128. Type the Netmask assigned to you by your ISP (if given)

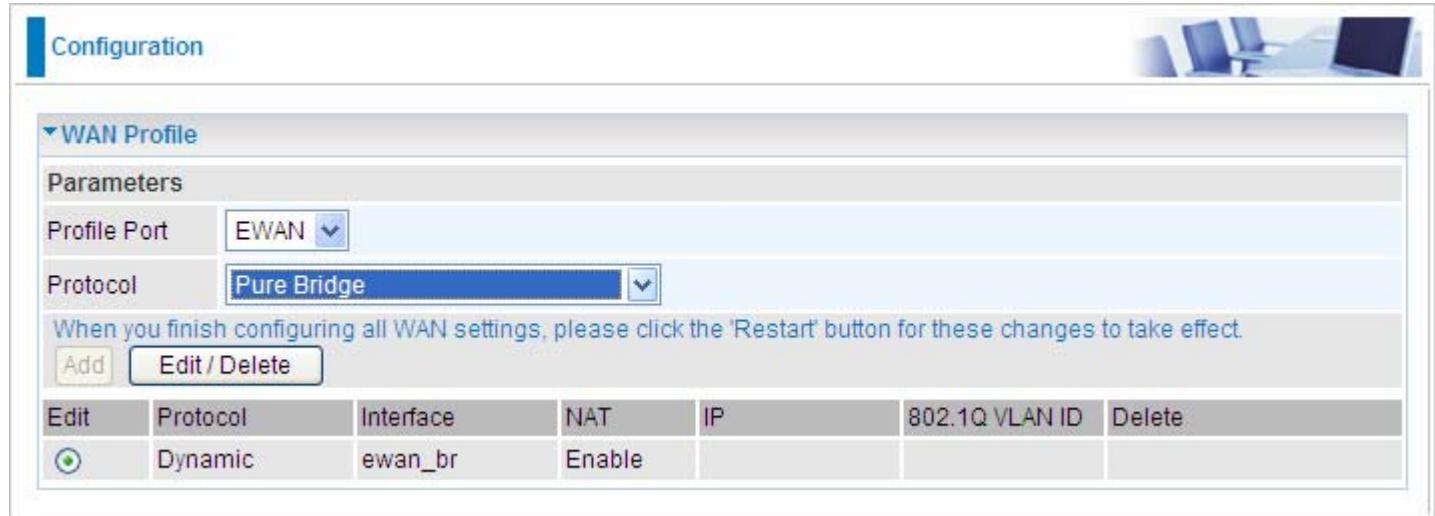
Gateway: Enter the IP address of the default gateway.

Obtain DNS: Select this check box to activate DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the Netmask.

Click Apply to confirm the settings.

Pure Bridge (EWAN)



Configuration

WAN Profile

Parameters

Profile Port: EWAN

Protocol: Pure Bridge

When you finish configuring all WAN settings, please click the 'Restart' button for these changes to take effect.

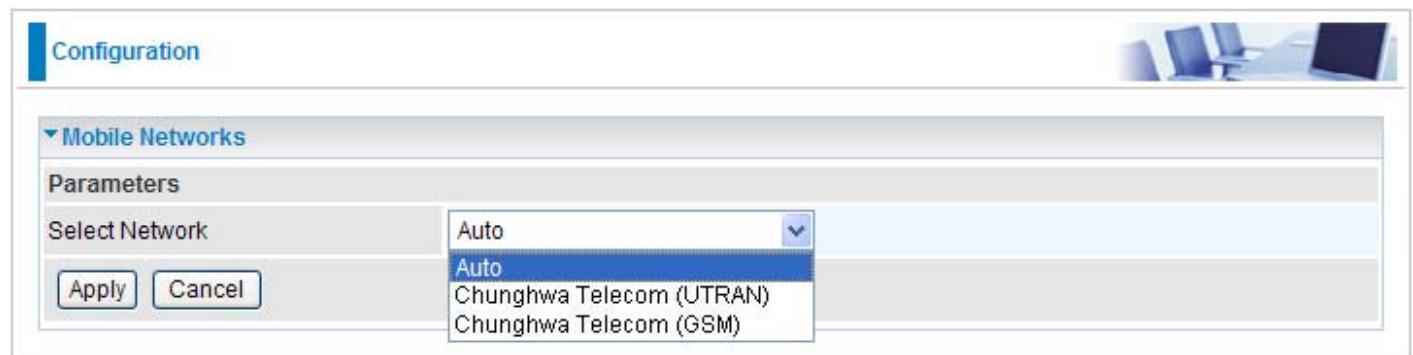
Add Edit / Delete

Edit	Protocol	Interface	NAT	IP	802.1Q VLAN ID	Delete
<input checked="" type="radio"/>	Dynamic	ewan_br	Enable			

Profile Port: Select EWAN as the profile port.

Protocol: Select Pure Bridge.

Mobile Networks



Configuration

Mobile Networks

Parameters

Select Network: Auto

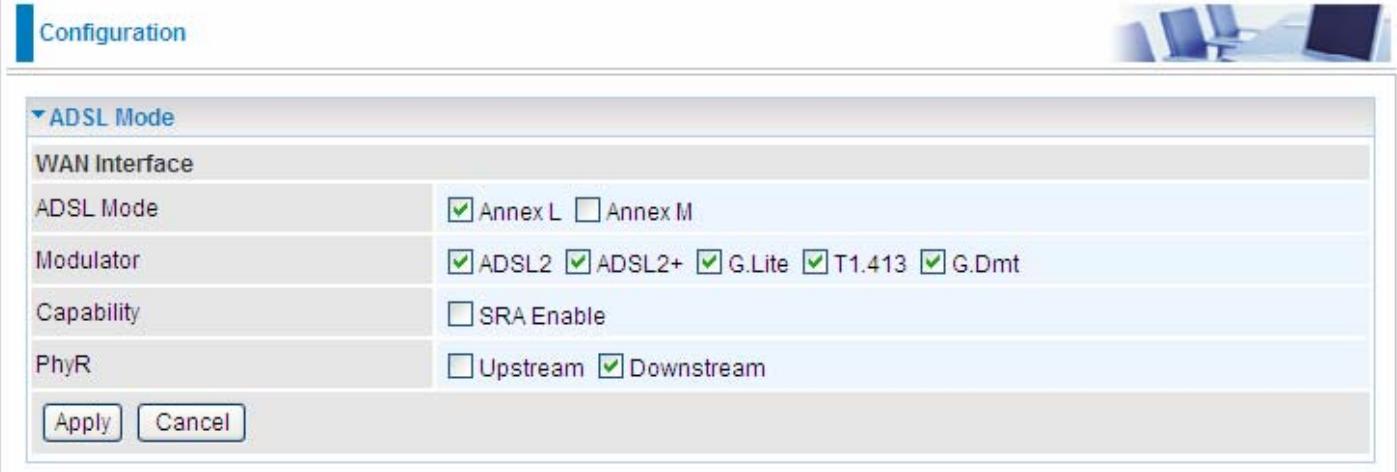
Apply Cancel

Auto
Chunghwa Telecom (UTRAN)
Chunghwa Telecom (GSM)

Select Network: Select the appropriate mobile network from the drop-down menu. Default is Auto.

Click Apply to confirm the settings.

ADSL Mode



WAN Interface	
ADSL Mode	<input checked="" type="checkbox"/> Annex L <input type="checkbox"/> Annex M
Modulator	<input checked="" type="checkbox"/> ADSL2 <input checked="" type="checkbox"/> ADSL2+ <input checked="" type="checkbox"/> G.Lite <input checked="" type="checkbox"/> T1.413 <input checked="" type="checkbox"/> G.Dmt
Capability	<input type="checkbox"/> SRA Enable
PhyR	<input type="checkbox"/> Upstream <input checked="" type="checkbox"/> Downstream

Apply **Cancel**

ADSL Mode: There are 2 modes: Annex L and Annex M that you can select for this connection.

Modulator: There are 5 modes: ADSL2, ADSL2+, G.Lite, T1.413 and G.Dmt that you can select for this connection.

SRA: select whether to enable SRA feature. **SRA**, short for **Seamless Rate Adaptation**, is a technology used to adapt the rate seamlessly without any influence to the working system, to assure of the quality of the ADSL system.

PhyR: An impulse noise protection technology to improve xDLS performance. It was based on your service provider. You can check Upstream and Downstream to improve Upstream or Downstream communication performance.

Click Apply to confirm the settings.

System

There are 9 items within the System section: [Time Zone](#), [Firmware Upgrade](#), [Backup/Restore](#), [Restart](#), [User Management](#), [Mail Alert](#), [SMS Alert](#), [Syslog](#) and [Diagnostics Tools](#).

Time Zone

Configuration

Time Zone

Parameters

Time Zone	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Local Time Zone (+-GMT Time)	(GMT) Greenwich Mean Time	
SNTP Server IP Address	192.43.244.18 129.6.15.29	128.138.140.44 216.218.192.202
Daylight Saving	<input checked="" type="checkbox"/> Automatic	
Resync Period	1440 minutes	



Apply Cancel

The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the most current time from an SNTP server outside your network. Choose your local time zone from the drop down menu. To apply the selected local time zone, click Enable and click the Apply button. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

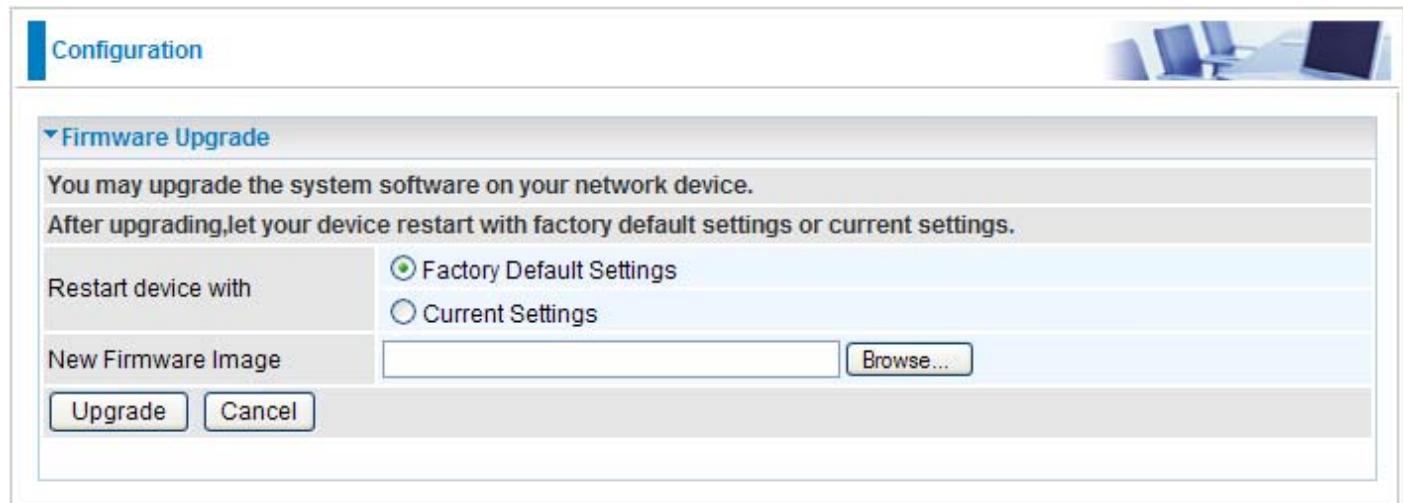
Daylight Saving is also known as Summer Time Period. Many places in the world adapt it during summer time to move one hour of daylight from morning to the evening in local standard time. Check Enable box to set your local time.

Resync Period (in minutes) is the periodic interval the router will wait before it re-synchronizes the router's time with that of the specified SNTP server. In order to avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible - at the absolute minimum every few hours or even days.

Click Apply to confirm the settings.

Firmware Upgrade

Your router's firmware is the software that enables it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software that runs in your router. Thus, by upgrading the newly improved version of the firmware allows you the advantage to use newly integrated features.



Configuration

Firmware Upgrade

You may upgrade the system software on your network device.

After upgrading, let your device restart with factory default settings or current settings.

Restart device with:

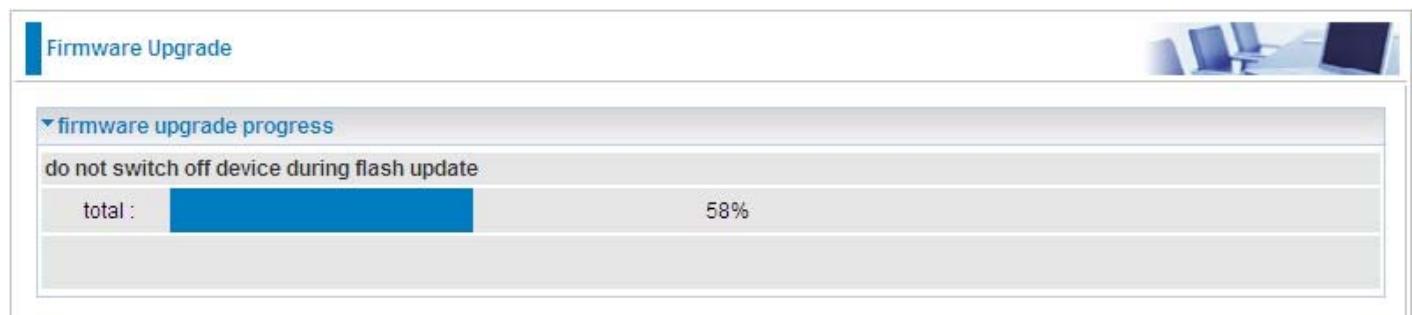
Factory Default Settings
 Current Settings

New Firmware Image:

Factory Default Settings: If select this setting, the device will reboot to restore the parameters of all its applications to its default values.

Current Settings: If select this setting, the device will reboot and retain the customized settings of all applications.

Click on Browse to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware to your router.



Firmware Upgrade

firmware upgrade progress

do not switch off device during flash update

total :  58%

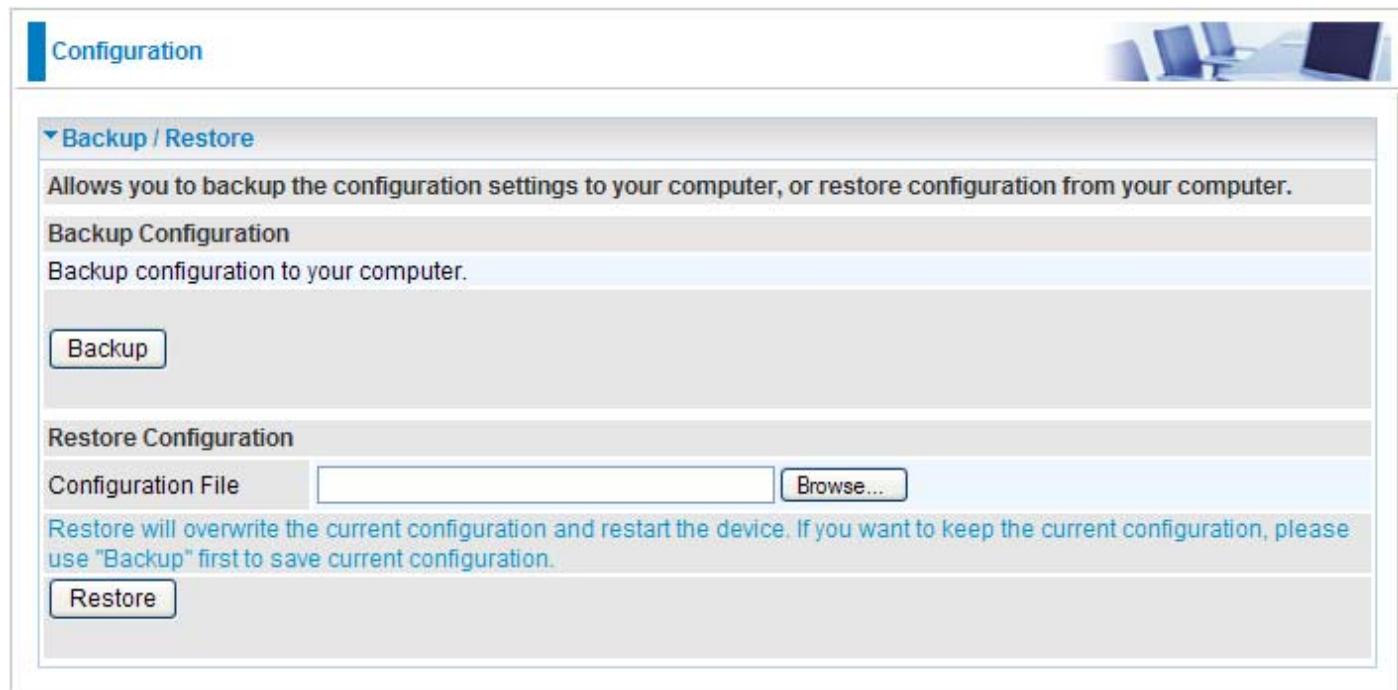


Warning

DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

Backup / Restore

These functions allow you to save a backup of the current configuration of your router to a defined location on your PC, or to restore a previously saved configuration. This is useful if you wish to experiment with different settings, knowing that you have a backup in hand in case any mistakes occur. It is advisable that you backup your router configuration before making any changes to your router configuration.



Configuration

Backup / Restore

Allows you to backup the configuration settings to your computer, or restore configuration from your computer.

Backup Configuration

Backup configuration to your computer.

Backup

Restore Configuration

Configuration File [Browse...](#)

Restore will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.

Restore

Backup Configuration

Press Backup Settings to select where on your local PC you want to store your setting file. You may also want to change the name of the file when saving if you wish to keep multiple backups.

Restore Configuration

Press Browse to select a file from your PC to restore. You should only restore your router setting that has been generated by the Backup function which is created with the current version of the router firmware. Settings files saved to your PC should not be manually edited in any way.

Select the settings files you wish to use, and press Restore to load the setting into the router. Click Restore to begin restoring the configuration and wait for the router to restart before performing any actions.

 8%'." data-bbox="56 698 936 837"/>

Restore Configuration

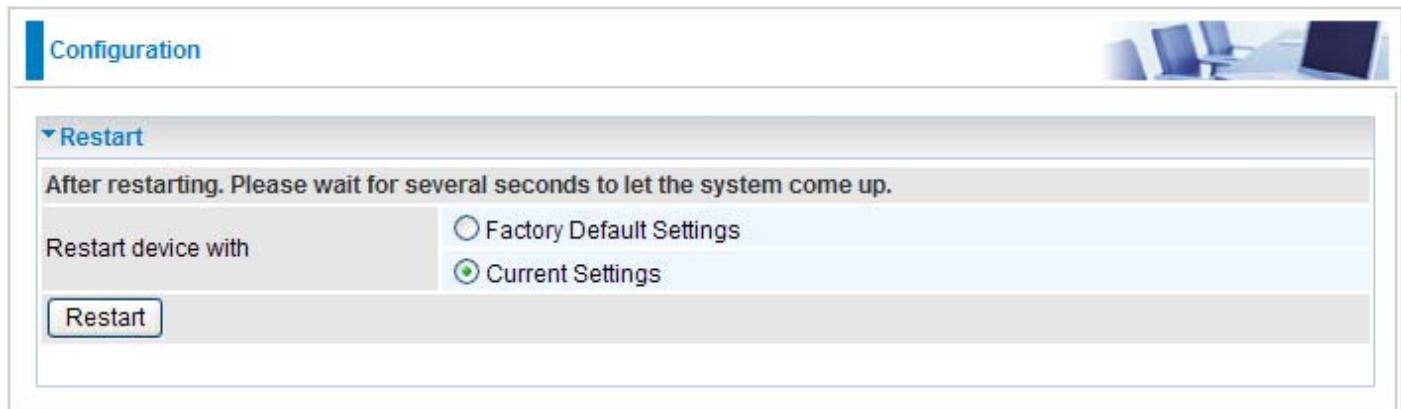
restore config progress

do not switch off device during flash update

total : 8%

Restart

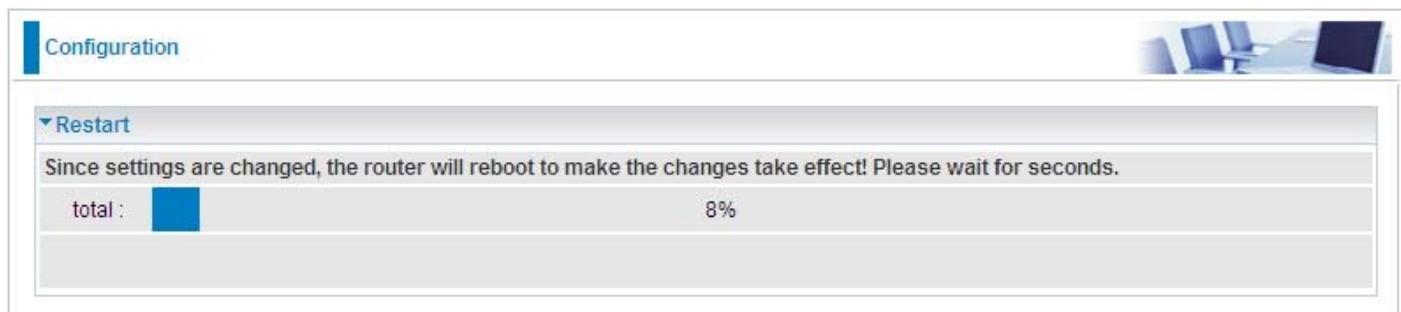
There are 2 options for you to choose from before restarting the 7800GZ(L) device. You can either choose to restart your device to restore it to the Factory Default Settings or to restart the device with your current settings applied. Restarting your device to Factory Default Setting will be useful especially after you have accidentally changed your settings that may result in undesirable outcome.



If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings.

Click Restart with option Current Settings to reboot your router (and restore your last saved configuration).

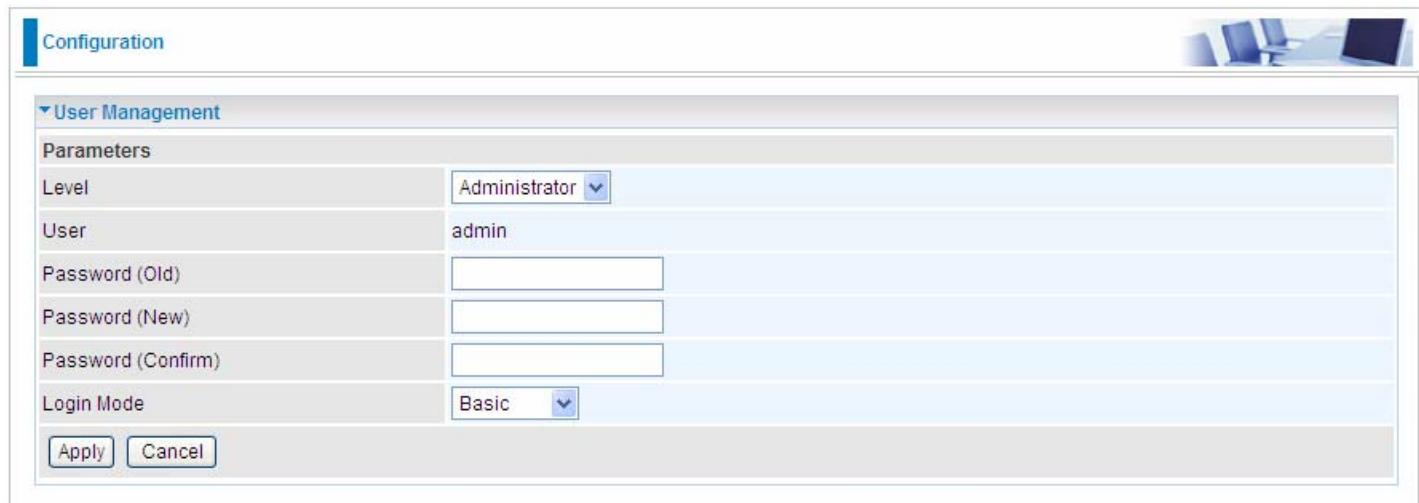
After selecting the type of setting you want the device to restart with, click the Restart button to initiate the process. After restarting, please wait several minutes to let the selected setting applied to the system.



You may also reset your router to factory settings by holding the small Reset pinhole button more than 1 second on the back of your router.

User Management

In order to prevent unauthorized access to your router configuration interface, it requires all users to login with a username and password. Three user levels are provided here. Each user level there's a default provided password. You must access the router with the appropriate username and password. Here the corresponding passwords are allowed to change. To change your password, simply enter the old password in the Old Password blank. Then enter your new password in the New Password and Confirm Password blanks provided. When this is done, press Apply to save changes.



Parameters	
Level	Administrator
User	admin
Password (Old)	
Password (New)	
Password (Confirm)	
Login Mode	Basic

Level: select which level you want to change password to. There are three default levels.

- ① **Administrator:** the root user, corresponding default username and password are admin and admin respectively.
- ① **Advanced:** username for the remote user to login, corresponding default username and password are support and support respectively.
- ① **Basic:** username for the general user, corresponding default username password are user and user respectivley.

User: display the username.

Password (Old): Enter the old password.

Password (New): Enter the new password.

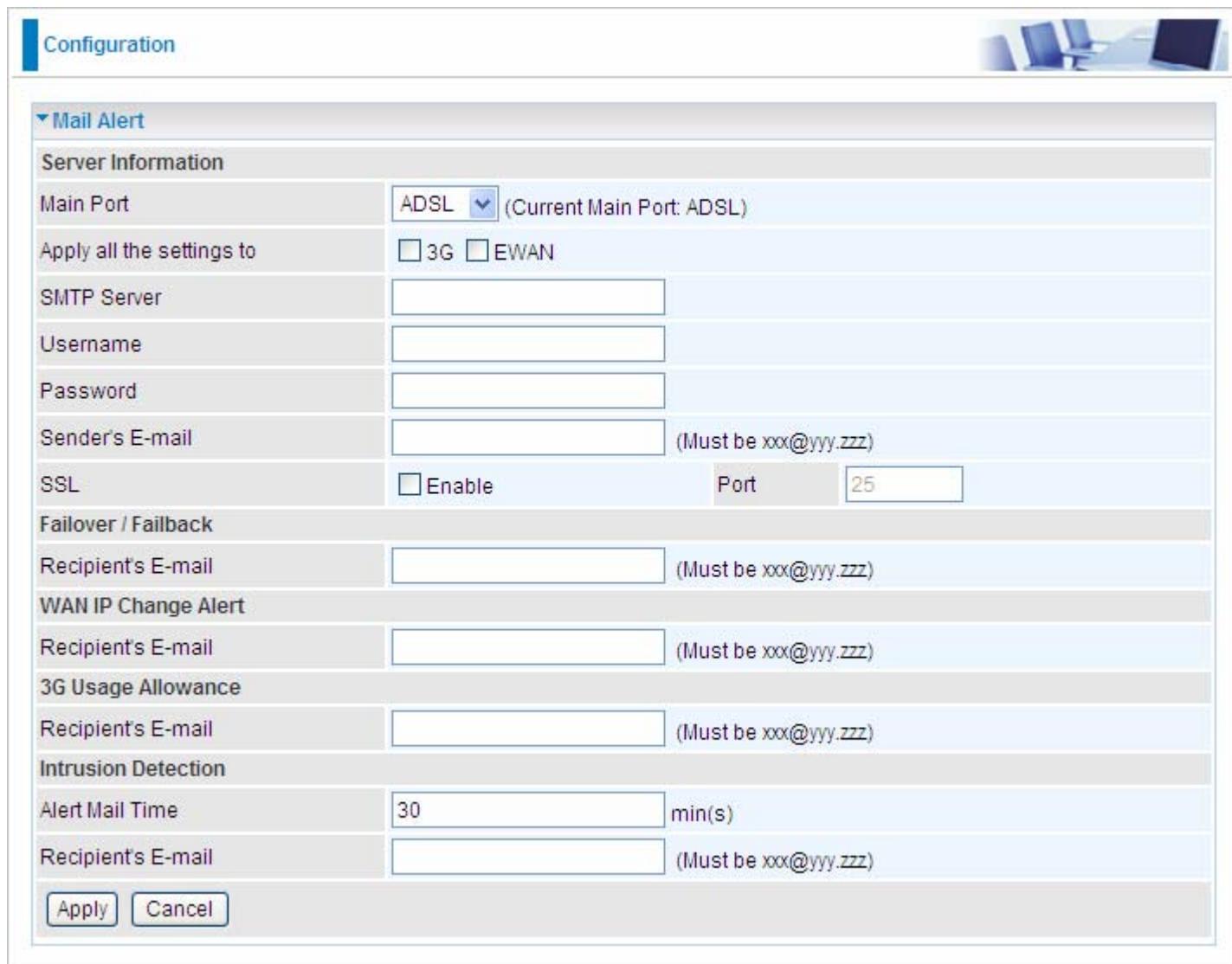
Password (Confirm): Enter again the new password to confirm.

Login Mode: choose to login to which Web GUI configuration page, Basic or Advanced. Basic will lead you to [Basic configuration](#) page, Advanced will lead you to [Advanced configuration](#) page.

Click Apply to apply your new settings.

Mail Alert

Mail alert is designed to keep system administrator or other relevant personnel alerted of any unexpected events that might have occurred to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained



Configuration

Mail Alert

Server Information

Main Port: ADSL (Current Main Port: ADSL)

Apply all the settings to: 3G EWAN

SMTP Server: [Text Input]

Username: [Text Input]

Password: [Text Input]

Sender's E-mail: [Text Input] (Must be xxx@yyy.zzz)

SSL: Enable Port: 25

Failover / Fallback

Recipient's E-mail: [Text Input] (Must be xxx@yyy.zzz)

WAN IP Change Alert

Recipient's E-mail: [Text Input] (Must be xxx@yyy.zzz)

3G Usage Allowance

Recipient's E-mail: [Text Input] (Must be xxx@yyy.zzz)

Intrusion Detection

Alert Mail Time: 30 min(s)

Recipient's E-mail: [Text Input] (Must be xxx@yyy.zzz)

Buttons: Apply, Cancel

Main Port: Choose the main port to be configured.

Apply all the settings to: Apply the settings for the current port to the other two ports.

SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

SSL: Enable the option and input your port number if your email is encrypted by SSL.

Recipient's Email (Failover / Fallback): Enter the email address that will receive the alert message once a computer / network server failover occurs.

Recipient's Email (WAN IP Change Alert): Enter the email address that will receive the alert

message once a WAN IP change has been detected.

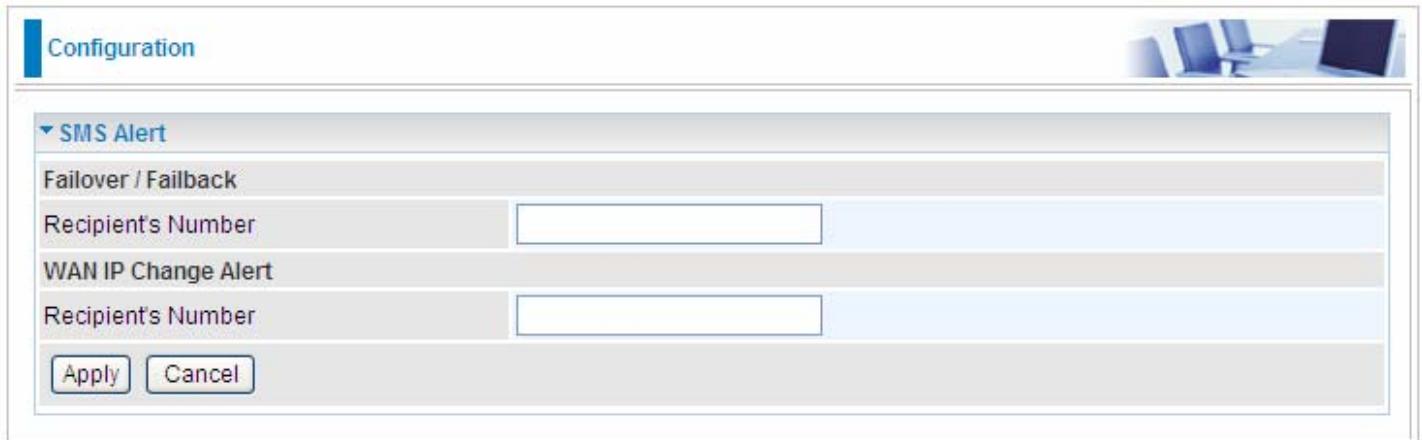
Recipient's Email (3G Usage Allowance): Enter the email address that will receive the alert message once the 3G over Usage Allowance occurs.

Alert Mail Time (intrusion Detection): the interval for sending alert mail.

Recipient's Email (intrusion Detection): Enter the email address that will receive the alert message once the intrusion is detected.

SMS Alert

SMS alert, similar to Mail Alert, is designed to keep system administrator or other relevant personnel alerted of any unexpected events that might have occurred to the network computers or server for monitoring efficiency. But instead of informing by Email, related persons can get the information via the short message on their phones sent by this device when WAN was changed to failover / fallback mode or WAN IP was changed



Recipient's Number (Failover / Failback): type the phone number which you want the person to get the information sent by this device once a computer / network server failover occurs.

Recipient's Number (WAN IP Change Alert): type the phone number which you want the person to get the information sent by this device once an IP change has been detected.

Syslog



Configuration

Syslog

Parameters

Remote Server

Server IP Address

Server UDP Port

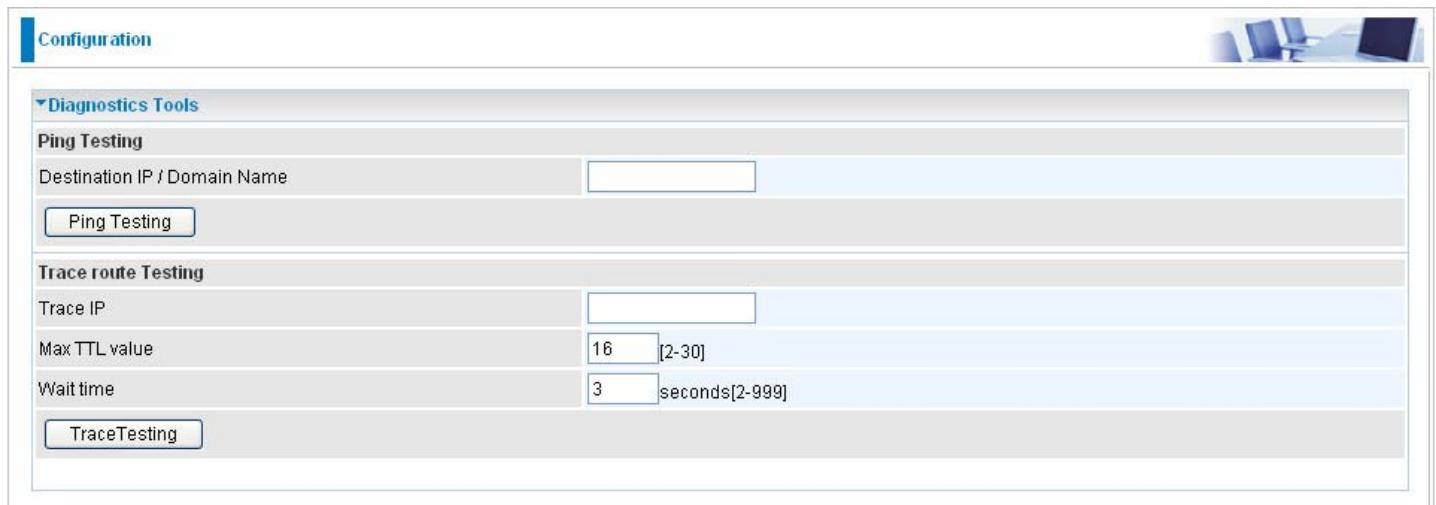
Apply Cancel

Remote Server: Specify the server that is used to save the device's syslog.

Server IP Address: The IP address of remote server.

Server UDP Port: The UDP Port of remote server.

Diagnostics Tools



Configuration

Diagnostics Tools

Ping Testing

Destination IP / Domain Name

Ping Testing

Trace route Testing

Trace IP

Max TTL value [2-30]

Wait time seconds [2-999]

TraceTesting

Destination IP / Domain Name: Input the IP or domain name to be tested.

Trace IP: Input IP to be traced.

Firewall

Listed are the items under the Firewall section: [Packet Filter](#), [Ethernet MAC Filter](#), [Wireless MAC Filter](#), [Intrusion Detection](#), [Block WAN PING](#) and [URL Filter](#).

Packet Filter

Packet filtering enables you to configure your router to block specific internal / external users (IP address) from Internet access, or disable specific service requests (Port number) to / from the Internet. This configuration program allows you to set up different filter rules for different users based on their IP addresses or their network Port number. The relationship among all filters is “or” operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

Order	Rule Name	Internal IP Address	External IP Address	Protocol	Internal Port	External Port	Direction	Action	Time Schedule	Delete
	Default	Any	Any	Any	Any	Any	outgoing	forward	Always On	

Rule Name: User defined description for entry identification. The maximum name length is 32 characters, and then can choose an application that they want from the listbox.

Internal IP Address / External IP Address: This is the Address-Filter used to allow or block traffic to/rom particular IP address(es). Input the range you want to filter out. If you leave these four fields empty or enter 0.0.0.0, it means any IP address.

Protocol: Specify the packet type (TCP, UDP, TCP/UDP, RAW, Any) that the rule applies to. Select TCP if you wish to search for the connection-based application service on the remote server using the port number. Or select UDP if you want to search for the connectionless application service on the remote server using the port number. Only when **RAW** is selected, then you can type the protocol number to identify the protocol that you want the filter applies to. When **Any** is selected, it means the filter will applies to any protocol.

Protocol Number: when **RAW** is selected in **Protocol** field, then type the specific protocol number here.

Action: If a packet matches this filter rule, forward (allows the packets to pass) or drop (disallow the packets to pass) this packet.

Internal Port: This Port or Port Range defines the ports allowed to be used by the Remote/WAN to connect to the application. Default is set from range 1 ~ 65535. It is recommended that this option be configured by an advanced user.

External Port: This is the Port or Port Range that defines the application.

Direction: Determine whether the rule is for outgoing packets or for incoming packets.

Time Schedule: A self defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Log: Select Enable for this option if you will like to capture the logs for this Packet filter policy.

Add: Click this button to add a new packet filter rule and the added rule will appear at the bottom table.

Edit: Check Edit next to the item you wish to edit, and then change parameters as desired. Complete it by press "Edit/Delete".

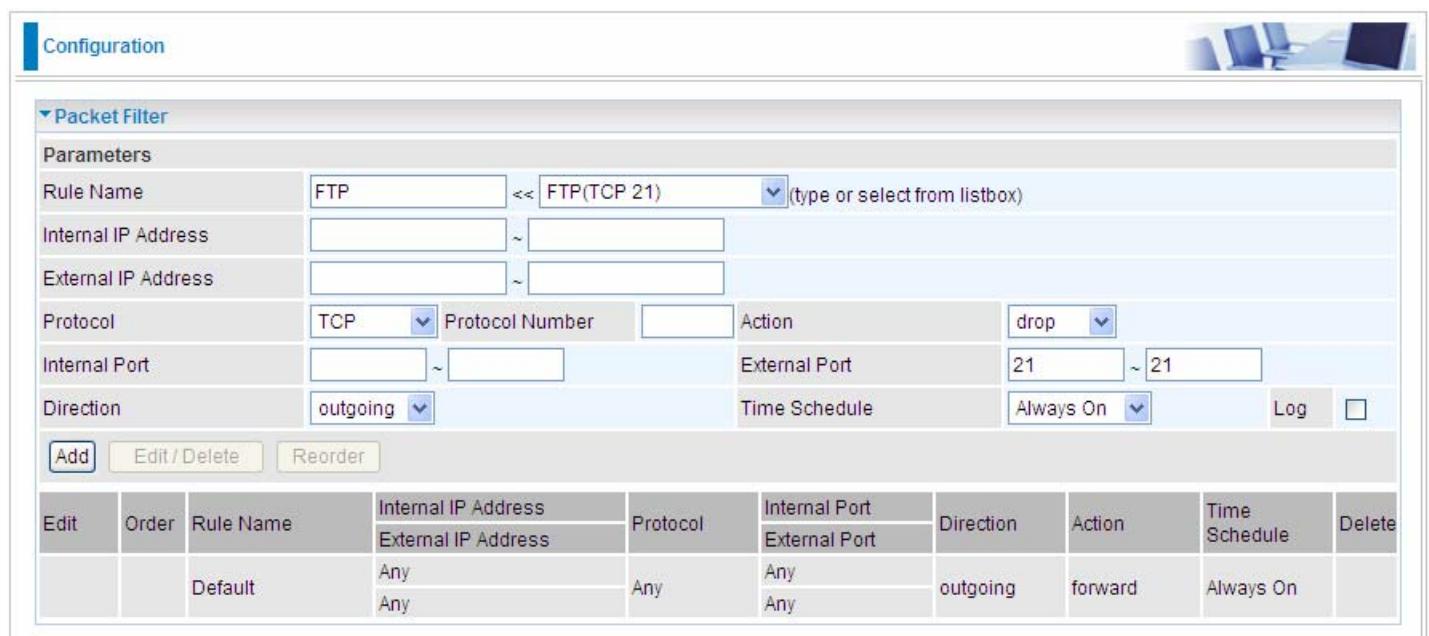
Delete: Check Delete next to the item you wish to delete, and press "Edit/Delete" to remove this rule.

Reorder: Be aware that packet filtering parameters appear in priority order i.e. the first one takes precedence over all other rules. There is a sort function next to the Rule Name column, you can move the rule to higher or lower priority by clicking the Order arrow, and press "Reorder" to save the new priority.

Creating a rule

Select or type a rule name, set other parameters as needed, then press Add. (two examples as follows)

FTP:



The screenshot shows a configuration interface for a packet filter. The top navigation bar includes 'Configuration' and a 'Logout' button. The main panel is titled 'Packet Filter' and contains the following fields:

Parameters	
Rule Name	FTP << FTP(TCP 21) (type or select from listbox)
Internal IP Address	~
External IP Address	~
Protocol	TCP
Internal Port	~
External Port	21 ~ 21
Direction	outgoing
Action	drop
Time Schedule	Always On
Log	<input type="checkbox"/>

Below these fields are three buttons: 'Add', 'Edit / Delete', and 'Reorder'. The 'Add' button is highlighted. The 'Reorder' button has a downward arrow icon. The 'Edit / Delete' button has an upward arrow icon.

At the bottom is a table showing the current rules:

Edit	Order	Rule Name	Internal IP Address	Protocol	Internal Port	Direction	Action	Time Schedule	Delete
		Default	Any	Any	Any	outgoing	forward	Always On	

Allowing_Any (allowing any incoming packets to be forwarded in):

Configuration

Packet Filter

Parameters

Rule Name	Allowing_Any	--select--	(type or select from listbox)
Internal IP Address	~		
External IP Address	~		
Protocol	Any	Protocol Number	Action
Internal Port	~		External Port
Direction	incoming		Time Schedule
		Always On	Log

Add Edit / Delete Reorder

Edit	Order	Rule Name	Internal IP Address	Protocol	Internal Port	Direction	Action	Time Schedule	Delete
			External IP Address		External Port				
○		FTP	Any	TCP	Any	outgoing	drop	Always On	<input type="checkbox"/>
			Any		21 ~ 21				
		Default	Any	Any	Any	outgoing	forward	Always On	<input type="checkbox"/>
			Any		Any				

Edit	Order	Rule Name	Internal IP Address	Protocol	Internal Port	Direction	Action	Time Schedule	Delete
			External IP Address		External Port				
○	↓	FTP	Any	TCP	Any	outgoing	drop	Always On	<input type="checkbox"/>
			Any		21 ~ 21				
○	↑	Allowing_Any	Any	Any	Any	incoming	forward	Always On	<input type="checkbox"/>
			Any		Any				
		Default	Any	Any	Any	outgoing	forward	Always On	<input type="checkbox"/>
			Any		Any				

① Editing and Deleting

Editing: Press the Edit radio button beside the item, and change the parameters, then press Edit/Delete to confirm.

Configuration

Packet Filter

Parameters

Rule Name	FTP	--select--	(type or select from listbox)
Internal IP Address	~		
External IP Address	~		
Protocol	TCP	Protocol Number	Action
Internal Port	~		External Port
Direction	outgoing		Time Schedule
		Always On	Log

Add Edit / Delete Reorder

Edit	Order	Rule Name	Internal IP Address	Protocol	Internal Port	Direction	Action	Time Schedule	Delete
			External IP Address		External Port				
○	↓	FTP	Any	TCP	Any	outgoing	drop	Always On	<input type="checkbox"/>
			Any		21 ~ 21				
		Allowing_Any	Any	Any	Any	incoming	forward	Always On	<input type="checkbox"/>
			Any		Any				
		Default	Any	Any	Any	outgoing	forward	Always On	<input type="checkbox"/>
			Any		Any				

Deleting: Check the checkbox, press Edit/Delete, then the item will be removed.

<input type="button" value="Add"/> <input style="border: 2px solid red; border-radius: 10px; padding: 2px; width: 100px; height: 30px; margin-right: 10px;" type="button" value="Edit / Delete"/> <input type="button" value="Reorder"/>											
Edit	Order	Rule Name	Internal IP Address	Protocol	Internal Port	Direction	Action	Time Schedule	Delete		
			External IP Address		External Port						
<input type="radio"/>		FTP	Any	TCP	Any	outgoing	drop	Always On	<input checked="" type="checkbox"/>		
			Any		21 ~ 21						
<input type="radio"/>		Allowing_Any	Any	Any	Any	incoming	forward	Always On	<input type="checkbox"/>		
			Any		Any						
<input type="radio"/>		HTTP	Any	TCP	Any	outgoing	drop	Always On	<input type="checkbox"/>		
			Any		80 ~ 80						
<input type="radio"/>		RAW	Any	RAW	Any	incoming	forward	Always On	<input type="checkbox"/>		
			Any		Any						
Default			Any	Any	Any	outgoing	forward	Always On			
			Any								

① Reorder

When there are more than one Filter rule, you can reorder them to the priority you want. The former is prior to the latter one.

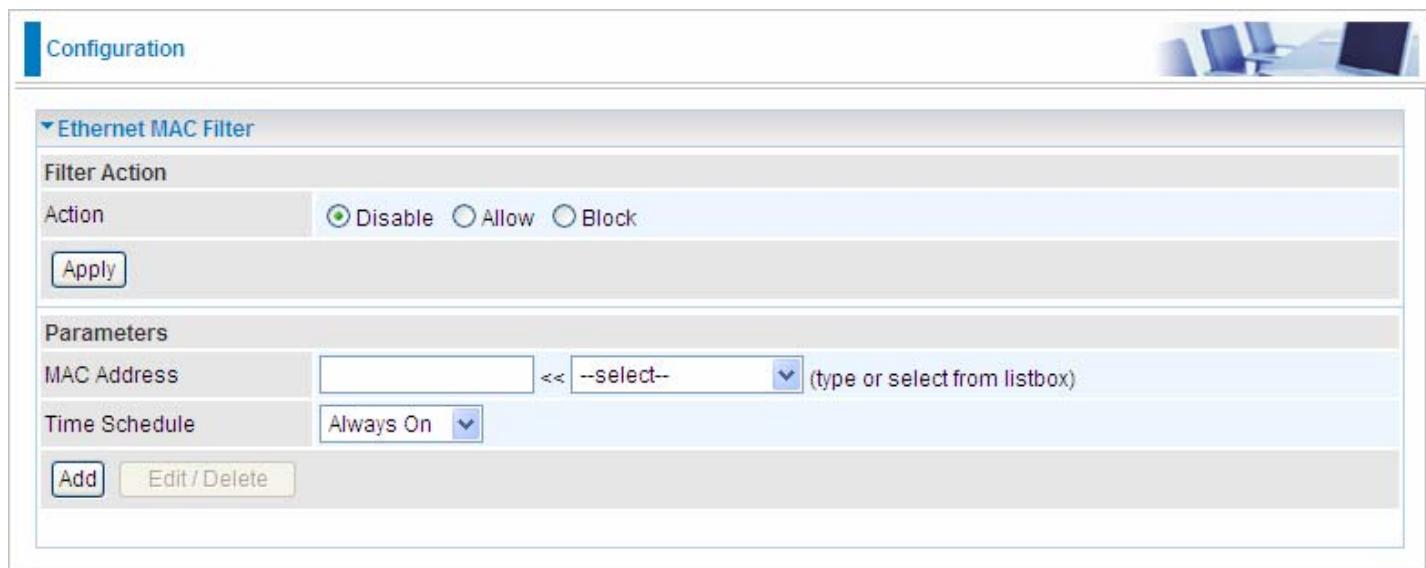
<input type="button" value="Add"/> <input type="button" value="Edit / Delete"/> <input type="button" value="Reorder"/>											
Edit	Order	Rule Name	Internal IP Address	Protocol	Internal Port	Direction	Action	Time Schedule	Delete		
			External IP Address		External Port						
<input type="radio"/>		FTP	Any	TCP	Any	outgoing	drop	Always On	<input type="checkbox"/>		
			Any		21 ~ 21						
<input type="radio"/>		Allowing_Any	Any	Any	Any	incoming	forward	Always On	<input type="checkbox"/>		
			Any		Any						
<input type="radio"/>		HTTP	Any	TCP	Any	outgoing	drop	Always On	<input type="checkbox"/>		
			Any		80 ~ 80						
<input type="radio"/>		RAW	Any	RAW	Any	incoming	forward	Always On	<input type="checkbox"/>		
			Any		Any						
Default			Any	Any	Any	outgoing	forward	Always On			
			Any								

Click or to change the priority of the filter, then press Reorder to confirm.

Ethernet MAC Filter

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the network to block specific machines from accessing your LAN.

There are no pre-defined MAC address filter rules, you can add the filter rules to you're your requirements.



The screenshot shows a software interface for configuring an Ethernet MAC Filter. The top navigation bar includes a 'Configuration' tab and a small network icon. The main panel is titled 'Ethernet MAC Filter'. The 'Filter Action' section contains a radio button group for 'Action' with 'Disable' selected, and buttons for 'Apply' and 'Edit / Delete'. The 'Parameters' section includes fields for 'MAC Address' (with a dropdown menu and a note '(type or select from listbox)') and 'Time Schedule' (set to 'Always On'). There are also 'Add' and 'Edit / Delete' buttons.

The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Filter Action

Action: Select an action for MAC Filter. This feature is disabled by default. Check Allow or Block to activate the filter.

Parameters

MAC Address: Enter the Ethernet MAC addresses you wish to have the filter rule applied.

Time Schedule: A self defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Wireless MAC Filter

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the network to block specific machines from accessing your LAN.

There are no pre-defined MAC address filter rules, you can add the filter rules to you're your requirements.



Configuration

Wireless MAC Filter

Filter Action

Action Disable Allow Block

Apply

Parameters

MAC Address << --select-- (type or select from listbox)

Add Edit / Delete

The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Filter Action

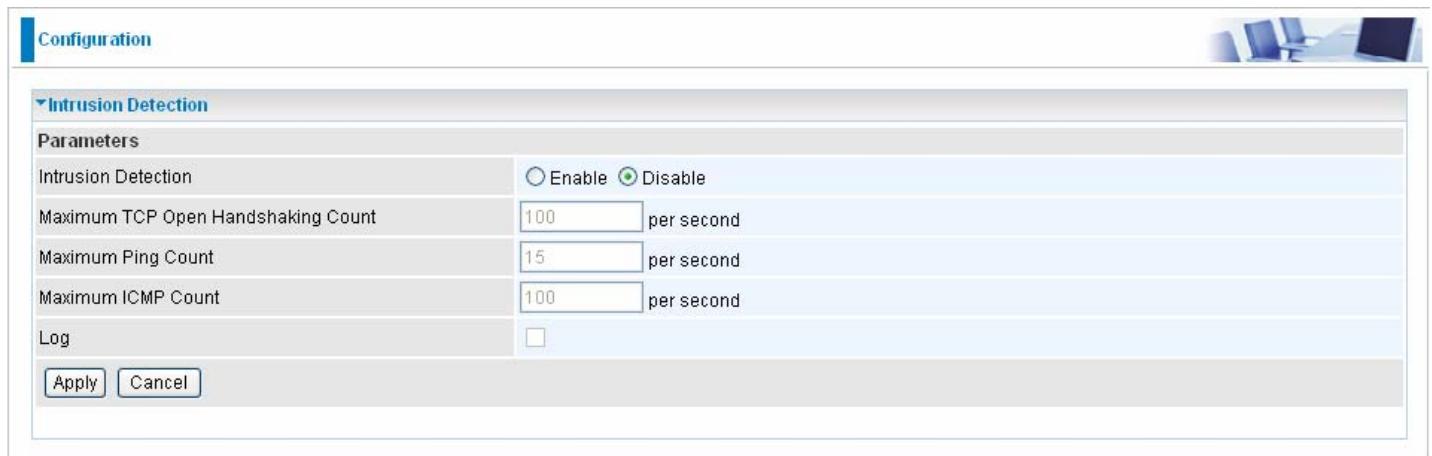
Action: Select an action for MAC Filter. This feature is disabled by default. Check Allow or Block to activate the filter.

Parameters

MAC Address: Enter the wireless MAC addresses you wish to have the filter applies.

Intrusion Detection

The router Intrusion Detection System (IDS) is used to detect hacker's attack and intrusion attempts from the Internet. If the IDS function of the firewall is enabled, inbound packets are filtered and blocked depending on whether they are detected as possible hacker attacks, intrusion attempts or other connections that the router determines to be suspicious.



Parameters	
Intrusion Detection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Maximum TCP Open Handshaking Count	100 per second
Maximum Ping Count	15 per second
Maximum ICMP Count	100 per second
Log	<input type="checkbox"/>

Max TCP Open Handshaking Count: This is a threshold value to decide whether a SYN Flood attempt is occurring or not. Default value is 100 TCP SYN per seconds.

Max PING Count: This is a threshold value to decide whether an ICMP Echo Storm is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

Max ICMP Count: This is a threshold to decide whether an ICMP flood is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

Log: Select Enable for this option if you will like to capture the logs for this Packet filter policy.

Block WAN Ping

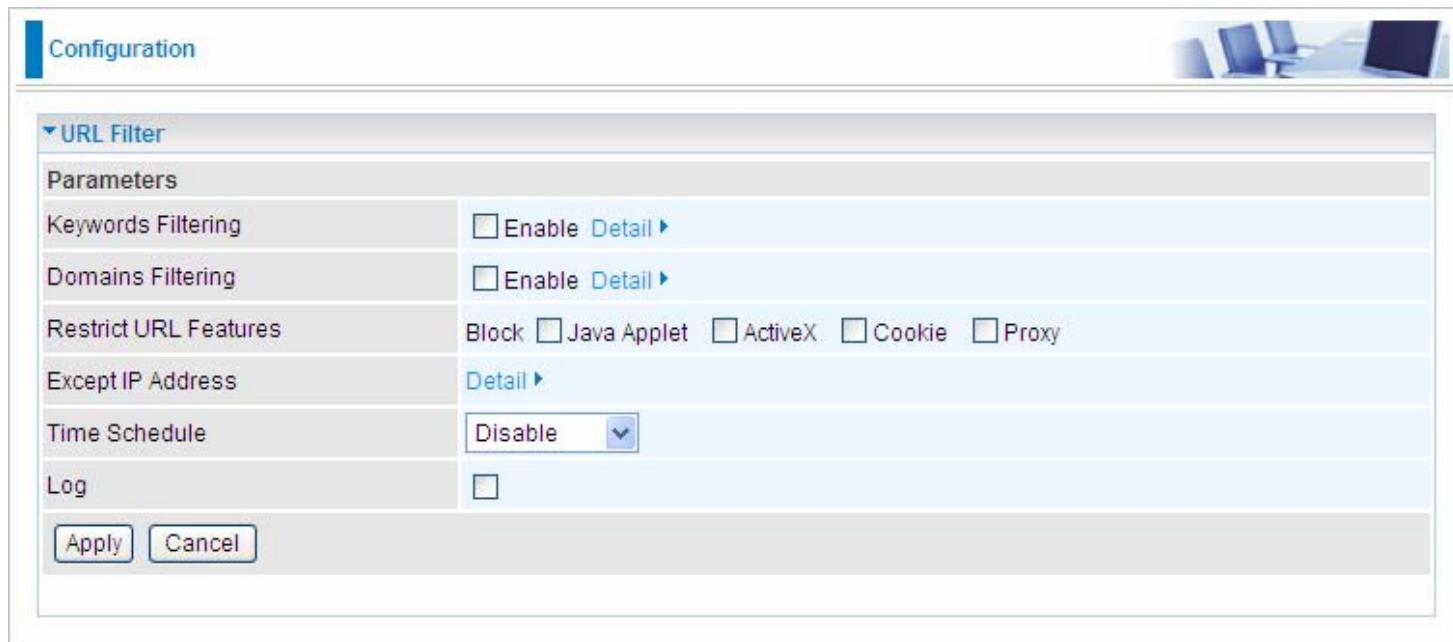
This feature is to be enabled when you want the public WAN IP address on your router not to respond to any ping command.



This feature is disabled by default. To activate the Block WAN PING feature, check the Enable box then click the Apply button.

URL Filter

The URL Filter is a powerful tool that can be used to limit access to certain URLs on the Internet. You can block web sites based on keywords or even block out an entire domain. Certain web features can also be blocked to grant added security to your network.



The screenshot shows the 'URL Filter' configuration page. It includes sections for 'Keywords Filtering', 'Domains Filtering', 'Restrict URL Features', 'Except IP Address', 'Time Schedule', and 'Log'. Each section has checkboxes and dropdown menus. At the bottom are 'Apply' and 'Cancel' buttons.

Keywords Filtering: Allow blocking against specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

Domains Filtering: This function checks the whole URL address but not the IP address against your list of domains to block or allow. If it is matched, the URL request will either be sent (Trusted) or dropped (Forbidden).

Restrict URL Features: Click **Block Java Applet** to filter web access with Java Applet components. Click **Block ActiveX** to filter web access with ActiveX components. Click **Block Cookie** to filter web access with Cookie components. Click **Block Proxy** to filter web proxy access.

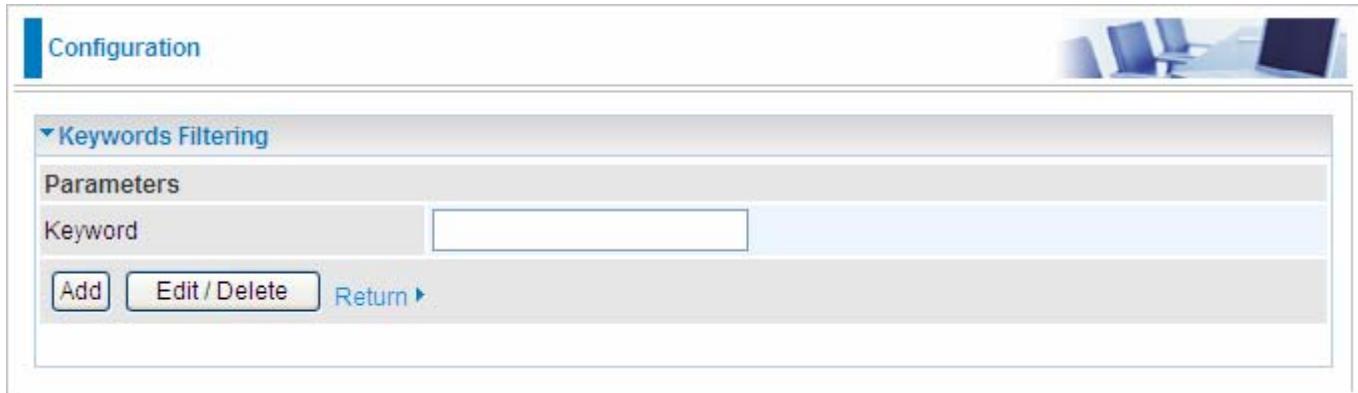
Exception List: You can input a list of IP addresses as the exception list for URL filtering.

Time Schedule: A self defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Log: Select Enable for this option if you will like to capture the logs for this URL filter policy.

Keywords filtering

Click the checkbox to enable this feature. To edit the list of filtered keywords, click **Details**.



Configuration

▼ Keywords Filtering

Parameters

Keyword

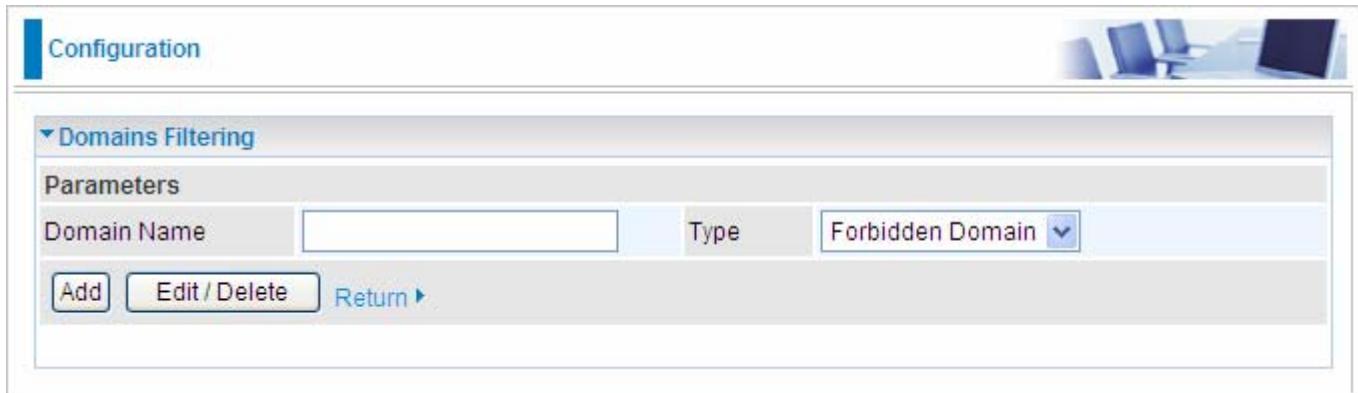
Type

Add Edit / Delete Return ▶

Enter a keyword to be filtered and click **Apply**. Your new keyword will be added to the filtered keyword listing.

Domains Filtering

Click the top checkbox to enable this feature. To edit the list of filtered domains, click **Details**.



Configuration

▼ Domains Filtering

Parameters

Domain Name

Type

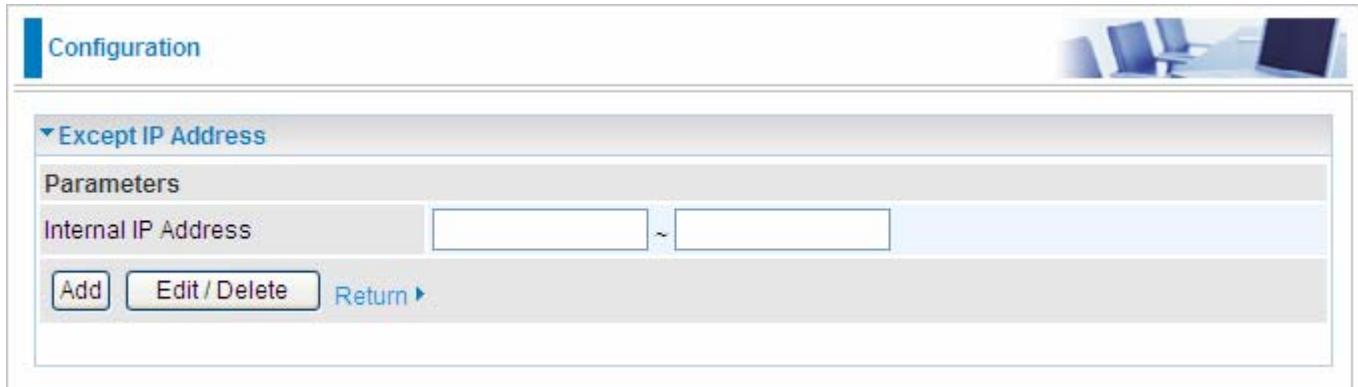
Type

Add Edit / Delete Return ▶

Enter a domain and select whether this domain is trusted or forbidden with the pull-down menu. Next, click **Apply**. Your new domain will be added to either the Trusted Domain or Forbidden Domain listing, depending on which you selected previously.

Except IP Address

You may also designate which IP addresses are to be excluded from these filters by adding them to the Exception List. To do so, click **Details**.



Configuration

▼ Except IP Address

Parameters

Internal IP Address ~

Type

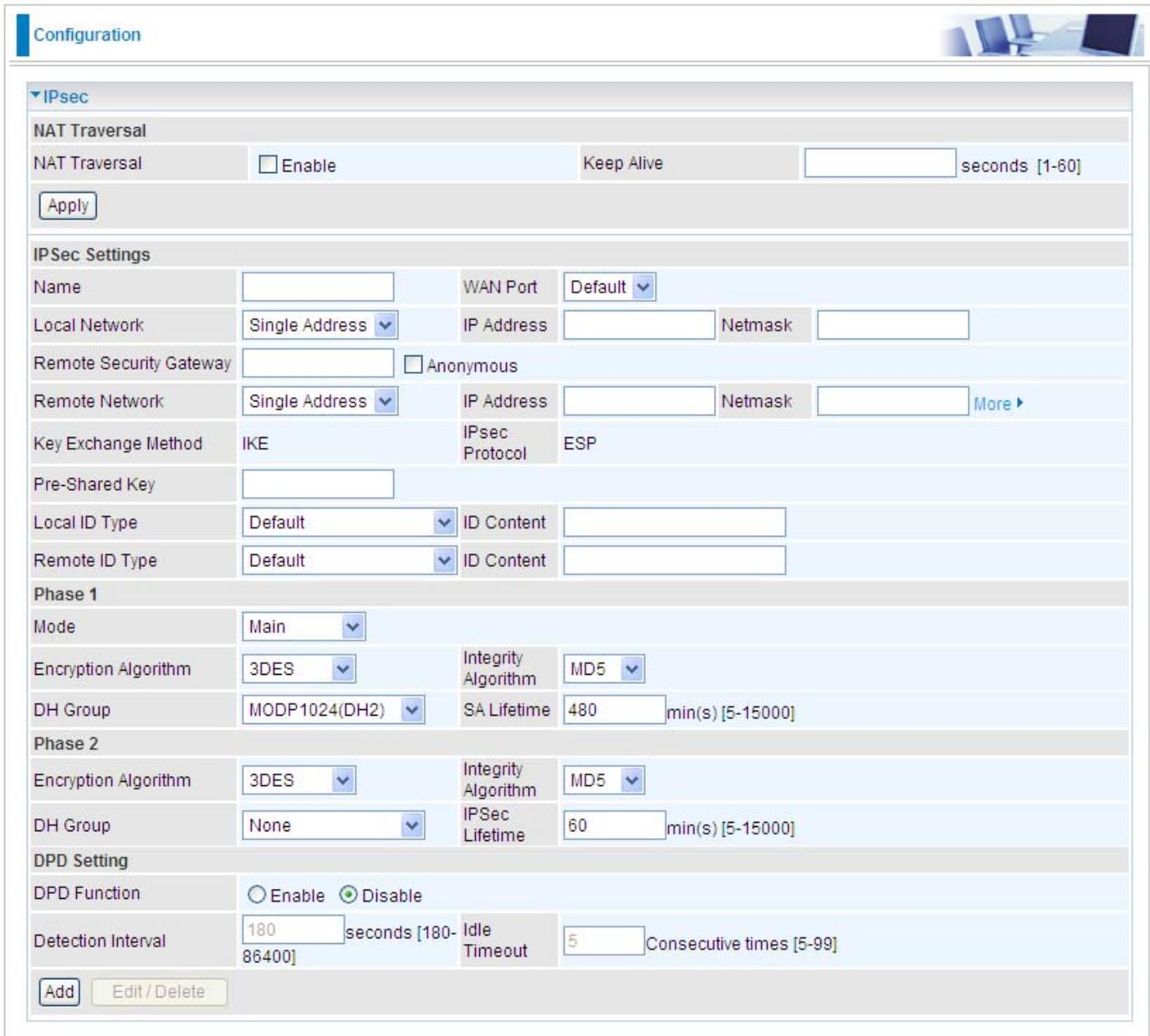
Add Edit / Delete Return ▶

Enter the except IP address. Click **Add** to save your changes. The IP address will be entered into the Exception List, and excluded from the URL filtering rules in effect.

VPN

Virtual Private Networks is ways to establish secured communication tunnels to an organization's network via the Internet. Your router supports the following: **IPSec, GRE**.

IPSec



The screenshot shows the 'IPSec' configuration page. It includes sections for 'NAT Traversal' (with 'Enable' and 'Keep Alive' fields), 'IPSec Settings' (with fields for 'Name', 'Local Network', 'Remote Security Gateway', 'Remote Network', 'Key Exchange Method', 'Pre-Shared Key', 'Local ID Type', and 'Remote ID Type'), 'Phase 1' (with fields for 'Mode', 'Encryption Algorithm', 'DH Group', and 'SA Lifetime'), 'Phase 2' (with fields for 'Encryption Algorithm', 'DH Group', and 'IPSec Lifetime'), 'DPD Setting' (with fields for 'DPD Function', 'Detection Interval', and 'Idle Timeout'), and a bottom row with 'Add' and 'Edit / Delete' buttons.

NAT Traversal

NAT Traversal: This directive enables use of the NAT-Traversal IPsec extension (NAT-T). NAT-T allows one or both peers to reside behind a NAT gateway (i.e., doing address- or port-translation).

Keep Alive: type the interval time(sec) for sending packets to keep the NAT Traversal alive.

Click Apply to save and apply your settings.

IPSec Settings

Name: A given name for the connection (e.g. "connection to office").

Local Network: Set the IP address or subnet of the local network.

Single Address: The IP address of the local host.

Subnet: The subnet of the local network. For example, IP: 192.168.1.0 with Netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1 (i.e. 192.168.1.1 through to 192.168.1.254).

Remote Secure Gateway: The IP address of the remote VPN device that is connected and establishes a VPN tunnel.

Anonymous: Enable any IP to connect in

Remote Network: Set the IP address or subnet of the remote network.

Single Address: The IP address of the remote host.

Subnet: The subnet of the remote network. For example, IP: 192.168.1.0 with Netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1 (i.e. 192.168.1.1 through to 192.168.1.254).

If remote peer supports multiple local subnets, you can click **More** to enter more subnets.

Remote Network	Single Address	IP Address	Netmask	More
IP Address / Netmask	1. None			
	2. None			
	3. None			

Key Exchange Method: Displays key exchange method.

Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Local ID Type and **Remote ID Type:** when the mode of phase 1 is aggressive, local and Remote ports can be identified by other IDs.

ID content: Enter ID content the name you want to identify when the Local and Remote Type are Domain Name; Enter ID content the email address you want to identify when the Local and Remote type are Email; Enter ID content IPv4 address you want to identify when the Local and Remote Type are IPv4 address.

Phase 1

Mode: Select IKE mode from the drop-down menu: Main or Aggressive. This IKE provides secured key generation and key management.

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: DES, 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

DES: Stands for Data Encryption Standard, it uses 56 bits as an encryption method.

3DES: Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.

AES: Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Integrity Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

MD5: A one-way hashing algorithm that produces a 128-bit hash.

SHA1: A one-way hashing algorithm that produces a 160-bit hash.

DH Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are 8 modes. MODP stands for Modular Exponentiation Groups.

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. Enter a value to issue an initial connection request for a new VPN tunnel. Default is 3600 seconds. A short SA time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

Phase 2

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: DES, 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

DES: Stands for Data Encryption Standard, it uses 56 bits as an encryption method.

3DES: Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.

AES: Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Integrity Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

MD5: A one-way hashing algorithm that produces a 128-bit hash.

SHA1: A one-way hashing algorithm that produces a 160-bit hash.

DH Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are 8 modes. MODP stands for Modular Exponentiation Groups.

IPSec Lifetime: Specify the number of minutes that IPSec will stay active before new encryption and authentication key will be exchanged. Enter a value to negotiate and establish secure authentication. Default is 3600 seconds. A short time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

DPD Setting

DPD Function: Check **Enable** to enable the function.

Detection Interval: The period cycle for dead peer detection. The interval can be 180~86400 seconds.

Idle Timeout: Auto-disconnect the IPSec connection after trying several consecutive times.

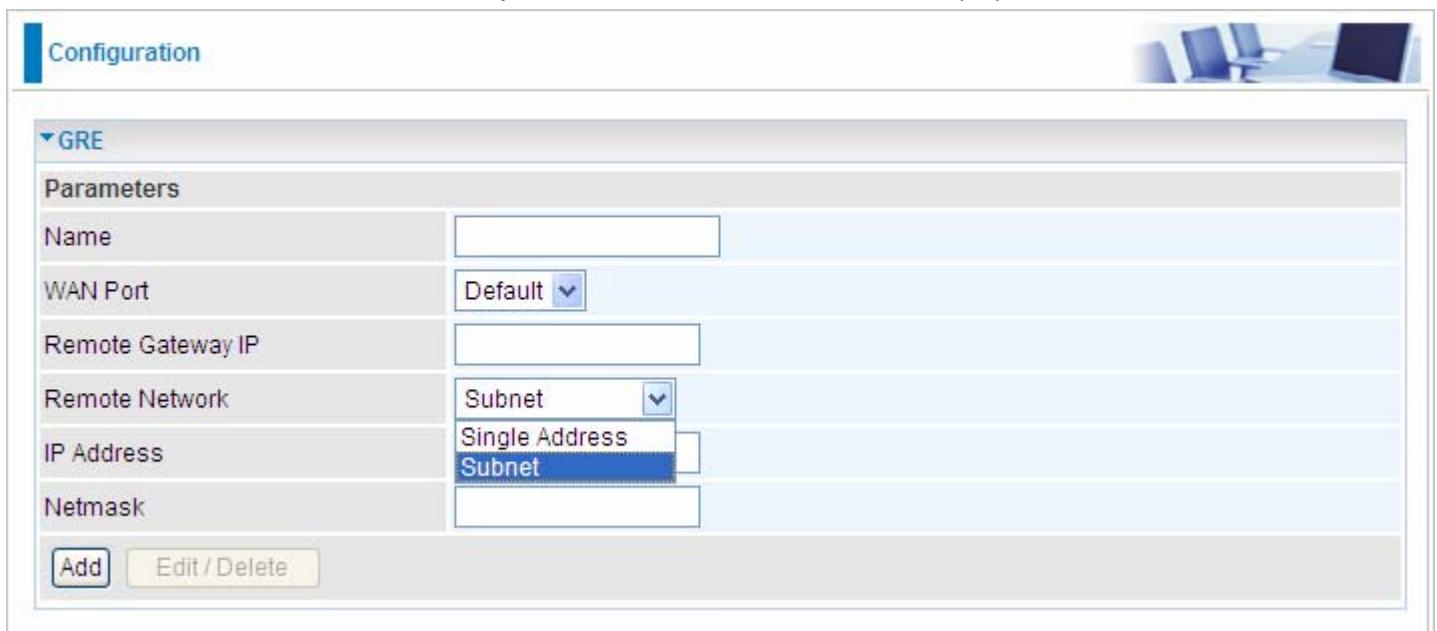
Add: Click this button to add a new IPSec entry and the added entry will appear at the bottom table.

Edit: Check Edit next to the item you wish to edit, and then change parameters as desired. Complete it by press “Edit/Delete”.

Delete: Check Delete next to the item you wish to delete, and press “Edit/Delete” to remove this entry.

GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocol packet types inside IP tunnels, creating a virtual point-to-point link to various brands of routers at remote points over an Internet Protocol (IP) internetwork.



The screenshot shows a 'Configuration' interface for 'GRE' parameters. The 'Parameters' section includes fields for 'Name' (empty), 'WAN Port' (set to 'Default'), 'Remote Gateway IP' (empty), 'Remote Network' (set to 'Subnet'), 'IP Address' (dropdown menu showing 'Single Address' and 'Subnet' with 'Subnet' selected), and 'Netmask' (empty). Below the form are 'Add' and 'Edit / Delete' buttons.

Name: A given name for the connection.

WAN Port: You can choose Default, ADSL, 3G or EWAN.

Remote Gateway IP: The IP address of the remote VPN device that is connected and establishes a VPN tunnel.

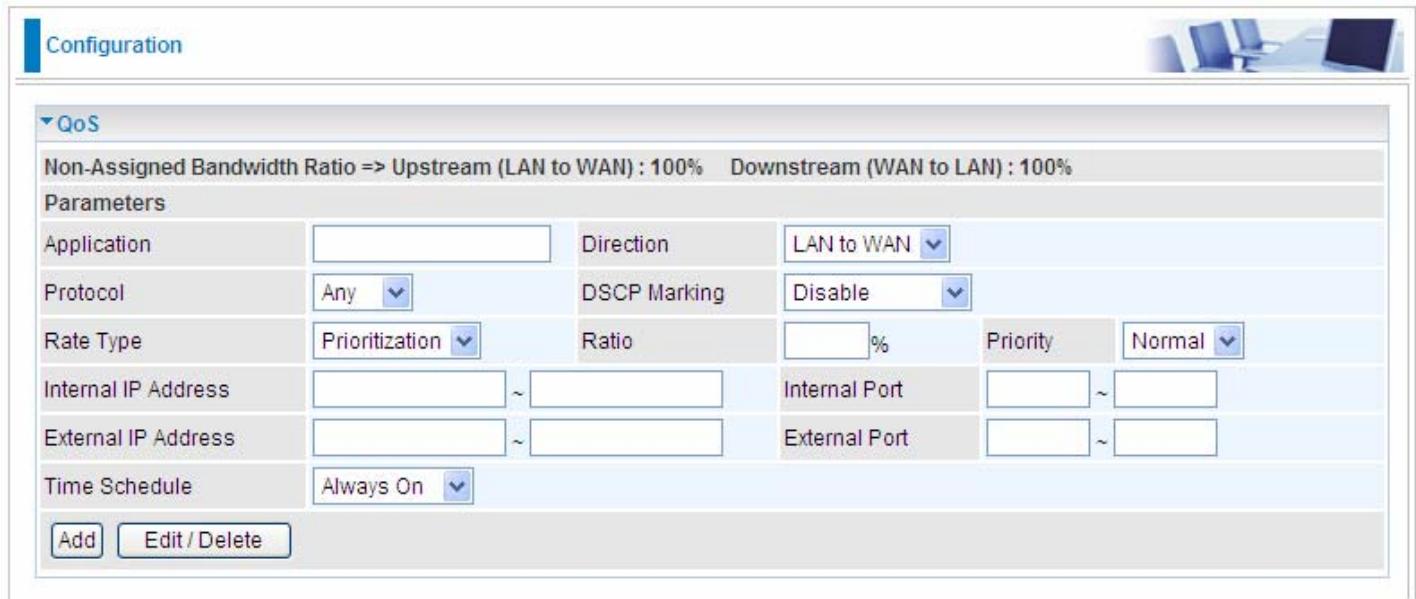
Remote Network: Set the IP address or subnet of the remote network.

IP Address: Enter the IP address of the remote network.

Netmask: Enter the netmask of the remote network.

QoS - Quality of Service

QoS helps you to control the data upload traffic of each application from LAN (Ethernet and/or Wireless) to WAN (Internet). It facilitates you the features to control the quality and speed of throughput for each application when the system is running with full upstream load.



The screenshot shows a configuration interface for Quality of Service (QoS). At the top, a blue bar labeled 'Configuration' is visible. Below it, a section titled 'QoS' is expanded. A message at the top of this section states: 'Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%'. The 'Parameters' section contains the following fields:

Application	<input type="text"/>	Direction	LAN to WAN
Protocol	Any	DSCP Marking	Disable
Rate Type	Prioritization	Ratio	<input type="text"/> %
Internal IP Address	<input type="text"/> ~ <input type="text"/>	Internal Port	<input type="text"/> ~ <input type="text"/>
External IP Address	<input type="text"/> ~ <input type="text"/>	External Port	<input type="text"/> ~ <input type="text"/>
Time Schedule	Always On		

At the bottom of the 'Parameters' section are two buttons: 'Add' and 'Edit / Delete'.

After clicking the QoS item, you can Add/Edit/Delete a QoS policy. This page will show the brief information for policies you have added or edited. This page will also display the total available (Non-assigned) bandwidth, in percentage, can be assigned.

Application: Assign a name that identifies the new QoS application rule.

Direction: Shows the direction mode of the QoS application.

- **LAN to WAN:** You want to control the traffic flow from the local network to the outside world (Upstream). You can assign the priority for the application or you can limit the your application used. e.g., you have a FTP server inside the local network and you want to have a limited traffic rate controlled by the QoS policy. So, you need to add a policy with LAN to WAN direction setting.
- **WAN to LAN:** Control Traffic flow from the WAN to LAN (Downstream). The connection maybe either issued from LAN to WAN or WAN to LAN.)

Protocol: Select the supported protocol from the drop down list.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the DSCP value.

Rate Type: You can choose Limited or Prioritization.

- **Limited (Maximum):** specify a limited data rate for this policy. It also is the maximal rate for this policy. When you choose Limited, type the Ratio proportion. As above FTP server example, you may want to “throttle” the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.
- **Prioritization:** to specify the rate type control for the rule to used. If you choose Prioritization for the rule, you parameter **Priority** would be available, you can set the priority for this rule.

Ratio: The rate percent in contrast to that on WAN interface given to each policy/application with limited rate type.

Priority: The priority given to each policy/application. Its default setting is set to Normal. You may adjust this setting to fit your policy / application.

Internal IP Address / External IP Address: This is used to classify the traffic of a specific range of internal/external IP address(es). Input the range you want to classify. If only the first IP block is filled, only that IP will be classified. If you leave these four fields empty, it means any classify IP address.

Internal Port: This is the Port Range that defines the ports allowed by the Remote/WAN to connect to the application. Default is set from range 1 ~ 65535. It is recommended that only advance user is to configure this feature.

External Port: This is the Port Range that defines the port of the application.

Time Schedule: A self defined time period. You may specify a time schedule for your QoS policy. For setup and detail, refer to Time Schedule section.

Note: *Make sure that the router(s) in the network backbone are capable to execute and check the DSCP throughout the QoS network.*

Example 1: Optimize Your Home Network with QoS

If you are actively engaged in using P2P and are afraid of slowing down internet access throughput of other users within your network, you can thus use QoS function to set different priorities for the different applications that members of your network will be using to avoid bandwidth traffic from getting overloaded.

Therefore, in order to assign the priority status of each application, we must first create a new QoS rule for each application.

The figures below show the different settings for assigning a High Priority status to Web Browsing, assigning limited rate for Email send & receive.

For Web Browsing

Configuration

QoS

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%

Parameters			
Application	HTTP	Direction	LAN to WAN
Protocol	TCP	DSCP Marking	Disable
Rate Type	Prioritization	Ratio	100%
Internal IP Address		Internal Port	
External IP Address		External Port	80
Time Schedule	Always On		
<input type="button" value="Add"/> <input type="button" value="Edit / Delete"/>			

For Mail Sending

Configuration

QoS

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%

Parameters										
Application	SMTP	Direction	LAN to WAN							
Protocol	TCP	DSCP Marking	Disable							
Rate Type	Limited	Ratio	40%							
Internal IP Address		Internal Port								
External IP Address		External Port								
Time Schedule	Always On									
<input type="button" value="Add"/> <input type="button" value="Edit / Delete"/>										
Edit	Application	Direction	Rate Type	Ratio	Priority	Internal IP Address	Protocol	Internal Port	Time Schedule	Delete
<input type="radio"/>	HTTP	LAN to WAN	Prioritization		High	Any	TCP	Any	Always On	<input type="checkbox"/>
						Any		80~80		

For Mail Receiving

Configuration

QoS

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 60% Downstream (WAN to LAN) : 100%

Parameters

Application	POP3	Direction	WAN to LAN
Protocol	TCP	DSCP Marking	Disable
Rate Type	Limited	Ratio	40 %
Internal IP Address		Internal Port	
External IP Address		External Port	
Time Schedule	Always On		

Edit	Application	Direction	Rate Type	Ratio	Priority	Internal IP Address	Protocol	Internal Port	Time Schedule	Delete
						External IP Address		External Port		
<input type="radio"/>	HTTP	LAN to WAN	Prioritization		High	Any Any	TCP	Any 80~80	Always On	<input type="checkbox"/>
<input type="radio"/>	SMTP	LAN to WAN	Limited	40%		Any Any	TCP	Any Any	Always On	<input type="checkbox"/>

QoS Rules created

Edit	Application	Direction	Rate Type	Ratio	Priority	Internal IP Address	Protocol	Internal Port	Time Schedule	Delete
						External IP Address		External Port		
<input type="radio"/>	HTTP	LAN to WAN	Prioritization		High	Any Any	TCP	Any 80~80	Always On	<input type="checkbox"/>
<input type="radio"/>	SMTP	LAN to WAN	Limited	40%		Any Any	TCP	Any Any	Always On	<input type="checkbox"/>
<input type="radio"/>	POP3	WAN to LAN	Limited	40%		Any Any	TCP	Any Any	Always On	<input type="checkbox"/>

Example 2: Optimize Your Home Network with QoS

If you are only using a specific PC for the P2P application, you can create a rule that has a low priority. In this way, P2P application will not congest the data transmission rate when there are other applications present.

Configuration

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%

Parameters

Application		Direction	LAN to WAN
Protocol	Any	DSCP Marking	Disable
Rate Type	Prioritization	Ratio	%
Internal IP Address		Internal Port	
External IP Address		External Port	
Time Schedule	Always On		

Edit	Application	Direction	Rate Type	Ratio	Priority	Internal IP Address	Protocol	Internal Port	Time Schedule	Delete
						External IP Address		External Port		
<input type="radio"/>	P2P	LAN to WAN	Prioritization		Low	Any	Any	Any	Always On	<input type="checkbox"/>
						Any		Any		

Virtual Server

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

In TCP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You also need to use port forwarding if you wish to host an online game server.

Example: List of some well-known and registered port numbers.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 1 to 65535, but only ports numbers 1 to 1023 are reserved for privileged services and are designated as “well-known ports” (Please refer to Table below). The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic or private ports, are numbered from 49152 through 65535.

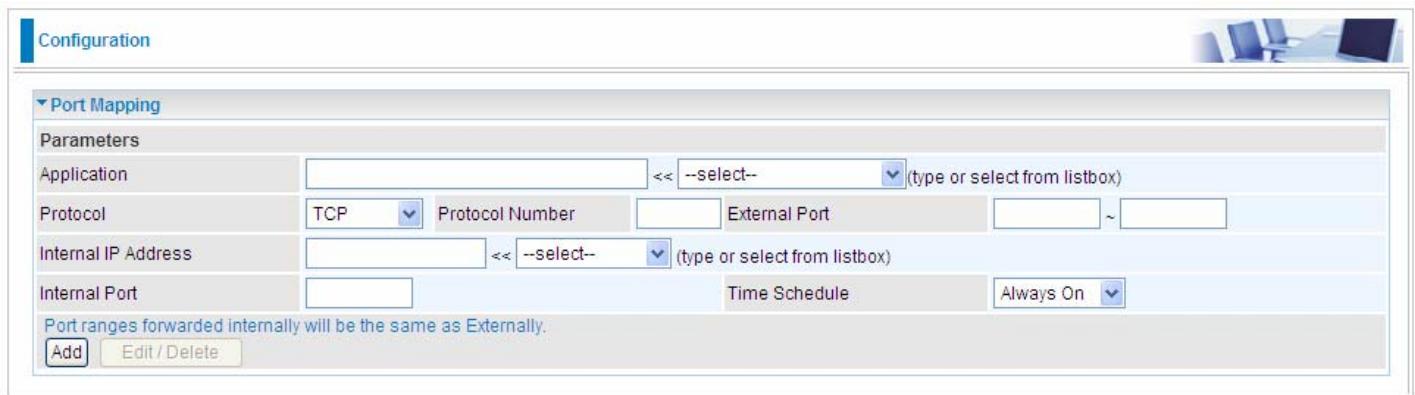
Examples of well-known and registered port numbers are shown below, for further information, please see IANA's website at: <http://www.iana.org/assignments/port-numbers>.

For help on determining which private port numbers are used by common applications on this list, please see the FAQs (Frequently Asked Questions) at <http://www.billion.com>.

Well-known and Registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	TELnet
25	TCP	SMTP (simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	Real Audio

Port Mapping



The screenshot shows a 'Port Mapping' configuration window. At the top, there's a 'Configuration' tab and a small graphic of a computer monitor. The main area is titled 'Port Mapping' and contains a 'Parameters' section with the following fields:

- Application:** A dropdown menu with a placeholder 'select' and a note '(type or select from listbox)'.
- Protocol:** A dropdown menu set to 'TCP' with a note '(type or select from listbox)'.
- Internal IP Address:** A dropdown menu with a placeholder 'select' and a note '(type or select from listbox)'.
- Internal Port:** An input field.
- Time Schedule:** A dropdown menu set to 'Always On'.

Below these fields is a note: 'Port ranges forwarded internally will be the same as Externally.' At the bottom of the window are two buttons: 'Add' and 'Edit / Delete'.

Application: Select the service you wish to configure.

Protocol: A protocol is automatically applied when an application is selected from the list-box or you may select a protocol type which you want. But when **RAW** is selected, you must set the protocol number to identify the protocol that the application utilizes.

Protocol Number: when **RAW** is selected in **Protocol** field, then type the specific protocol number (1~254) here.

External Port & Internal Port: Enter the public port number & range you wish to configure.

Internal IP Address: Enter the IP address of a specific internal server to which requests from the specified port is forwarded.

Add: Click to add a new virtual server rule. Click again and the next figure appears.

Edit: Check the Edit radio button to display the parameter of the selected application, then after changing the parameters click the "Edit/Delete" button to apply the changes.

Delete: To remove a port mapping application, check the Delete box of the selected application then click the "Edit/Delete" button.

Time Schedule: A self defined time period. You may specify a time schedule for your port mapping. For setup and detail, refer to Time Schedule section.

Since NAT acts as a "natural" Internet firewall, your router protects your network from accessed by outside users, as all incoming connection attempts point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a "virtual server". You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port23), SMTP (port 25), or POP3 (port 110). When an incoming access request the router for a specified port is received, it is forwarded to the corresponding internal server.

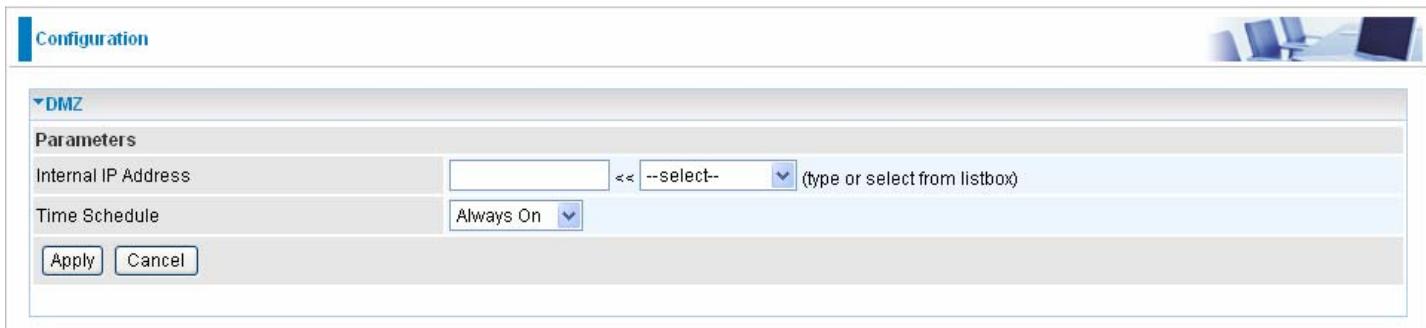
For example, if you set the port number 80 (Web/HTTP) to be mapped to the IP Address 192.168.1.2, then all incoming HTTP requests from outside users are forwarded to the local server(PC) with the IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

Edit	Application	Protocol	External Port	Internal IP Address	Internal Port	Time Schedule	Delete
<input checked="" type="radio"/>	FTP	TCP	21	192.168.1.25	21	Always On	<input type="checkbox"/>
<input checked="" type="radio"/>	HTTP	TCP	80	192.168.1.2	80	TimeSlot2	<input type="checkbox"/>

In addition to specifying the port number used, you also need to specify the protocol used. The protocol is determined by a particular application. Most applications use TCP or UDP, however you may also specify other protocols using the drop-down Protocol menu. Setting the protocol to “all” causes all incoming connection attempts using all protocols on all port numbers to be forwarded to the specified IP address.

DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets that do not use a port number which is already used by any other Virtual Server entries will first be checked by the Firewall and NAT algorithms before it is passed to the DMZ host. When this is done, press Apply to save the changes.



Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.



NOTE: Since outside users are able to connect to the PCs on your network, port mapping utilization imposes security implications. You are therefore advised to use specific Virtual Server entries just for those ports that your applications require.

One-to-One NAT

One-to-One NAT maps a specific private/local address to a global/public IP address.

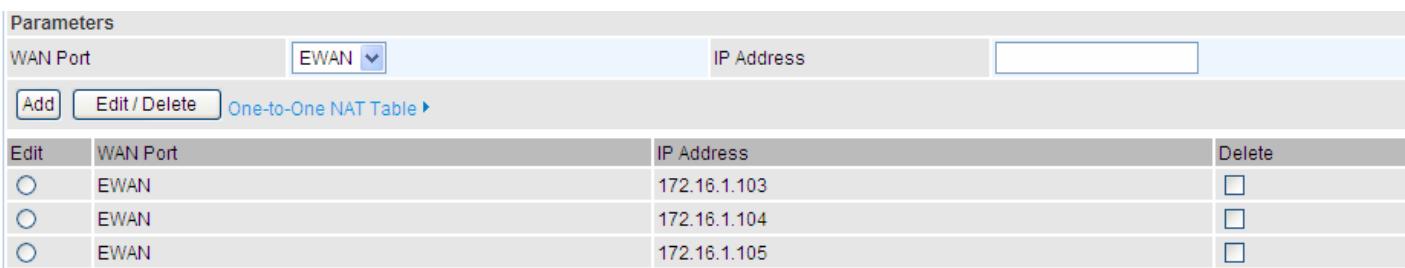
If you have multiple public/WAN IP address from your ISP, you are eligible for One-to-One NAT to utilize these IP addresses.



WAN IP Pool: select **Enable** to activate the feature and Click **Apply** to submit your configuration.

WAN Port: choose the WAN port you are going to configure multiple IPs for One-to-One NAT. for example, you have three available public IPs from 172.16.1.103-172.16.1.105 (internal test for instance), you can add these IPs respectively to the following IP Address field.

IP Address: Type each available WAN IPs to this field and Click Add to add respectively to show as below.



Then Click [One-to-One NAT Table](#) to go on distributing the WAN IP to the specific local IP.



Global IP Address: the set WAN IP, you can type manually or select if you have add to the list before.

Internal IP Address: set the concrete local IP you want to map to the WAN IP.

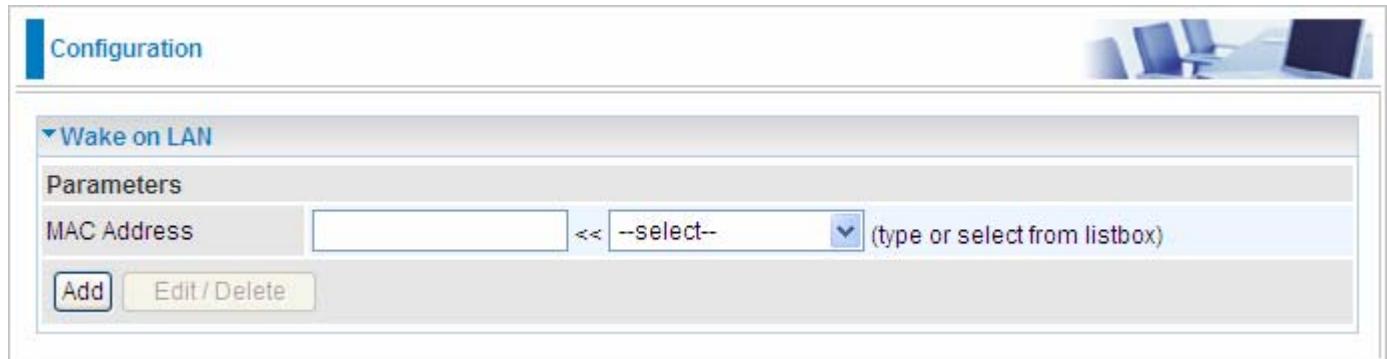
ALG

The ALG Controls enable or disable protocols over application layer.



Wake on LAN

This feature provides greater flexibility for users to turn on / boot the computer of the network from a remote site.



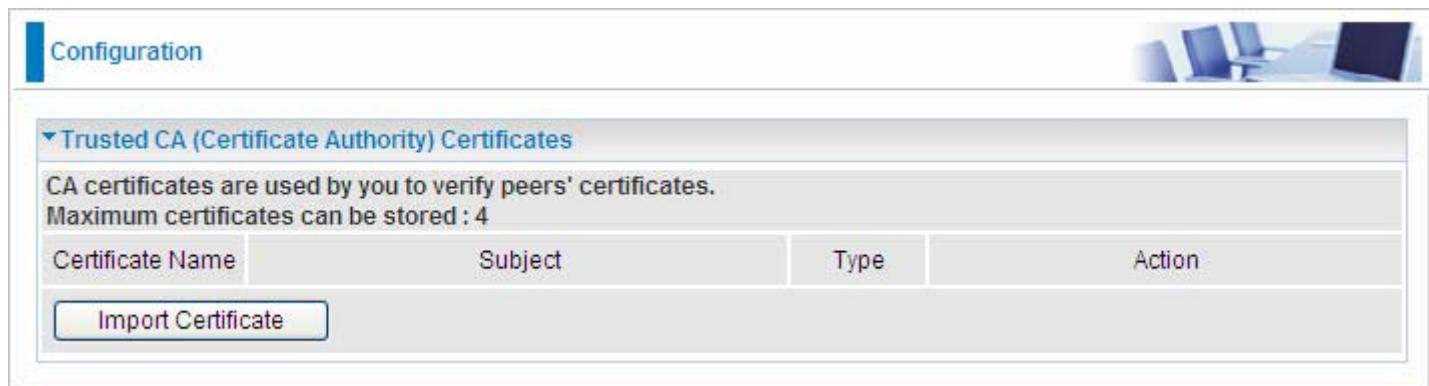
MAC Address: Enter the MAC address of the target computer or you can select the MAC address directly from the Select drop down menu on the right.

--select-- : You can select the MAC from this list.

Certificate

This feature is used for TR069 ACS Server authentication of the device used certificate, if necessary. If the imported certificate doesn't match the authorized certificate of the ACS Server, the device will have no access to the server.

Trusted CA



The screenshot shows a web-based configuration interface for managing Trusted CA (Certificate Authority) Certificates. The top navigation bar includes a 'Configuration' tab and a small graphic of a computer monitor. The main content area is titled 'Trusted CA (Certificate Authority) Certificates'. A sub-instruction states: 'CA certificates are used by you to verify peers' certificates. Maximum certificates can be stored : 4'. Below this, a table lists certificates with columns for 'Certificate Name', 'Subject', 'Type', and 'Action'. A prominent 'Import Certificate' button is located at the bottom left of the table area.

Certificate Name: the certificate identification name.

Subject: the certificate subject.

Type: the certificate type information. "ca", indicates that the certificate is a CA-signed certificate.

"self", indicates that the certificate is a certificate owner signed one.

"x.509", indicates the certificate is the one created and signed according to the definition of Public-Key System suggested by x.509.

Action:

■ **View:** view the certificate.

■ **Remove:** remove the certificate.

Click **Import Certificate** button to import your certificate.

Configuration

Import CA certificate

Parameters

Certificate Name	<input type="text"/>
Certificate	<pre>-----BEGIN CERTIFICATE----- <insert certificate here> -----END CERTIFICATE-----</pre>

Enter the certificate name and insert the certificate.

Configuration

Import CA certificate

Parameters

Certificate Name	<input type="text" value="acscert"/>
Certificate	<pre>-----BEGIN CERTIFICATE----- MIICyTCCAjKgAwIBAgIEOURomDANBgkqhkiG9w0BAQUFADAkMQswCQYDVQQGEwJD TjEVMBMGA1UEChMMQ0ZDQSBSb290IENBMB4XDTAwMDYxMjA0MDcwN1oXDTIwMDYx MjA0MDcwN1owJDELMakGA1UEBhMCQ04xFTATBgNVBAoTDENGQ0EgUm9vdCBDQTCB nzANBgkqhkiG9w0BAQEFAAOBJQAwgYkCgYEAwQf0h96iyMw0c+3ksNQxDX4AfXer 8W79sLYS1JtvDB1Dzon3+C/k1lyH5/Um5C0dy+XZo6j7ST4tSWR+F2K4t6E3BXtN ysy/rMrS2Hcm+t06XYuInJSzzMjb5EU7TPQB619WSWtHBTbCVMdM9ze6QSgXyhtE tAnvJFa4eJtoI/MCAwEAAAaOCAQYwggECMBEGCwCGSAGG+EIBAQQAwiABzBGBgNV HR8EPzA9MDugOaA3pDUwMzELMAkGA1UEBhMCQ04xFTATBgNVBAoTDENGQ0EgUm9v dCBDQTENMAgGA1UEAxMEQ1JMMTAzBgNVHRAEJDAlgA8yMDAwMDYxMjA0MDcwN1qB DzIwMjAwNjEyMDQzNzA2WjALBgNVHQ8EBAMCAQYwHwYDVR0jBBgwFoAUfxqihN9J Cd+XoKYCmug8dPvtzsMwHQYDVROOBByEFH8aooZ/SQnf16CmAproPHT77c7DMAwG A1UdEwQFMAMBAf8wHQYJKoZIhvZ9BOEABBAwDhsIVjUuMDo0LjADAgSQMA0GCSqG SIb3DQEBBQUAA4GBAACPC0WV3cQVjZKEiP3OSbKPzJn4gpetOZP+NeWvZ8LeeTgOy dg0LR0J9rGrIURj+JiMXmVG1DKEJAdrOeaKbzJDR6zuAer6iRmPpzDpDjaM16sSb yim2fxaBnW7Ns+fT1aZ3i+8q5MERi3eJaiyCOSJB1qPUeEkjm6JP75812e2C -----END CERTIFICATE-----</pre>

Click Apply to confirm your settings.

Configuration

Trusted CA (Certificate Authority) Certificates

CA certificates are used by you to verify peers' certificates.
Maximum certificates can be stored : 4

Certificate Name	Subject	Type	Action
acscert	C=CN/O=CFCA Root CA	ca	View Remove

[Import Certificate](#)

Time Schedule

The Time Schedule supports up to 16 time slots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allow the use of the Internet by users or applications.

Time Schedule correlates closely with router time. Since router does not have a real time clock on board, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server. Refer to Time Zone for details. Your router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.

Configuration

Time Schedule

Parameters

Name	<input type="text"/>	Day in a week	<input type="checkbox"/> Sun	<input type="checkbox"/> Mon	<input type="checkbox"/> Tue	<input type="checkbox"/> Wed	<input type="checkbox"/> Thu	<input type="checkbox"/> Fri	<input type="checkbox"/> Sat	
Start Time	00 <input type="button" value="▼"/> 00 <input type="button" value="▼"/>	End Time	00 <input type="button" value="▼"/> 00 <input type="button" value="▼"/>							
<input type="button" value="Edit / Clear"/>										
Edit	Name	Day in a week	Start Time	End Time	Clear					
<input type="radio"/>	TimeSlot1	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot2	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot3	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot4	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot5	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot6	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot7	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot8	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot9	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot10	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot11	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot12	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot13	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot14	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot15	smtwtf	08:00	18:00	<input type="checkbox"/>					
<input type="radio"/>	TimeSlot16	smtwtf	08:00	18:00	<input type="checkbox"/>					

Advanced

Configuration options within the Advanced section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

Here are the items within the **Advanced** section: [Static Route](#), [Static ARP](#), [Static DNS](#), [Dynamic DNS](#), [VLAN](#), [Device Management](#), [IGMP](#), [TR-069 client](#), [Remote Access](#) and [Web Access Control](#).

Static Route

With static route feature, you are equipped with the capability to control the routing of the all the traffic across your network. With each routing rule created, you can specifically assign the destination where the traffic will be routed to.



The screenshot shows a configuration interface for a static route. At the top, a blue header bar says "Configuration". Below it, a section titled "Static Route" is expanded. Under "Parameters", there are four input fields: "Destination" (empty), "Netmask" (empty), "Gateway" (empty), and "Interface" (a dropdown menu). Below these fields are two buttons: "Add" (highlighted in blue) and "Edit / Delete".

Destination: Enter the destination IP where the traffic is to be forwarded.

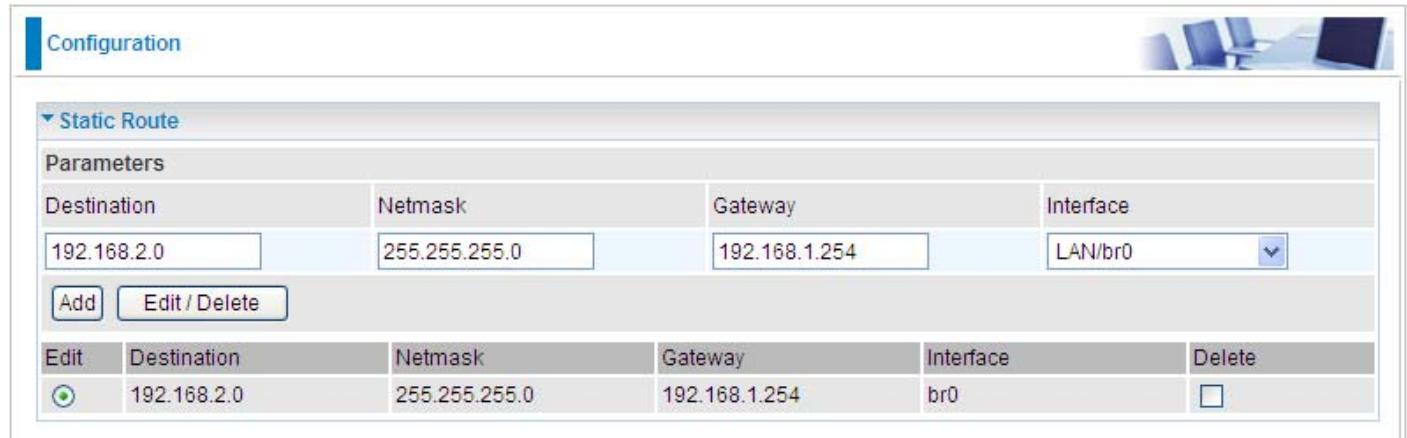
Netmask: Enter the Netmask of the destination.

Gateway: Enter the gateway address for the traffic.

Interface: Select an appropriate interface for the new routing rule from the drop down menu.

Click Add to confirm the settings.

Edit: Check the Edit radio button to display the parameter of the selected application, then after changing the parameters click the "Edit/Delete" button to apply the changes.



The screenshot shows the same configuration interface for a static route, but now with data entered. The "Destination" field contains "192.168.2.0", the "Netmask" field contains "255.255.255.0", the "Gateway" field contains "192.168.1.254", and the "Interface" dropdown is set to "LAN/br0". Below these fields are the "Add" and "Edit / Delete" buttons, with "Edit" being the active button. A table below shows the row for "192.168.2.0" with columns for Edit, Destination, Netmask, Gateway, Interface, and Delete. The "Edit" cell for this row is also highlighted in blue.

Edit	Destination	Netmask	Gateway	Interface	Delete
<input checked="" type="radio"/>	192.168.2.0	255.255.255.0	192.168.1.254	br0	<input type="checkbox"/>

Delete: To remove a static route entry, check the Delete box of the selected entry then click the "Edit/Delete" button.

Configuration

Static Route

Parameters

Destination	Netmask	Gateway	Interface
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="▼"/>

Edit	Destination	Netmask	Gateway	Interface	Delete
<input type="radio"/>	192.168.2.0	255.255.255.0	192.168.1.254	br0	<input checked="" type="checkbox"/>

Static ARP

This feature allows you to map the layer-2 MAC (Media Access Control) address that corresponds to the layer-3 IP address of the device.



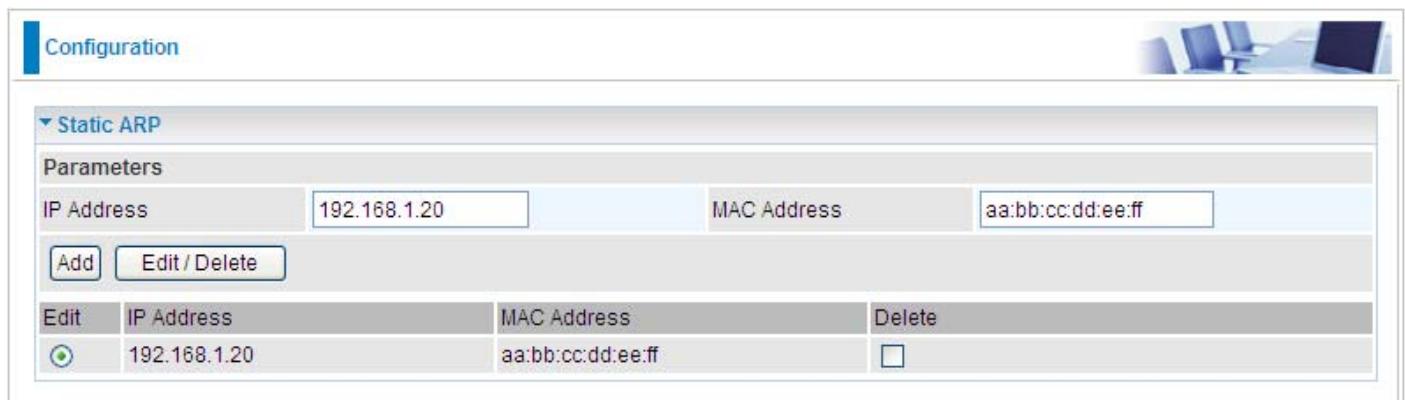
The screenshot shows a configuration interface for 'Static ARP'. At the top, there is a 'Configuration' tab and a small network icon. Below it, a 'Static ARP' section is expanded. The 'Parameters' section contains two input fields: 'IP Address' and 'MAC Address'. Below these fields are two buttons: 'Add' and 'Edit / Delete'. The entire interface is contained within a light gray box.

IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.

MAC Address: Enter the MAC address that corresponds to the IP address of the device.

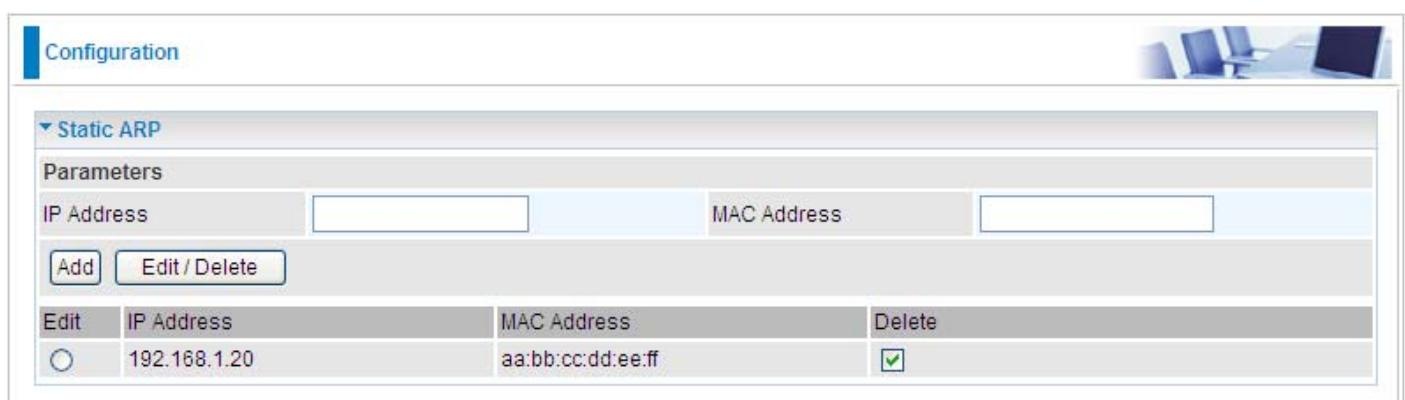
Click Add to confirm the settings.

Edit: Check the Edit radio button to display the parameter of the selected application, then after changing the parameters click the "Edit/Delete" button to apply the changes.



The screenshot shows the same configuration interface for 'Static ARP'. The 'Edit' button is highlighted in blue. Below the 'Edit' button, the IP address '192.168.1.20' and MAC address 'aa:bb:cc:dd:ee:ff' are displayed. A 'Delete' button is also visible. The entire interface is contained within a light gray box.

Delete: To remove a static ARP entry, check the Delete box of the selected entry then click the "Edit/Delete" button.



The screenshot shows the configuration interface for 'Static ARP'. The 'Edit / Delete' button is highlighted in blue. Below it, the IP address '192.168.1.20' and MAC address 'aa:bb:cc:dd:ee:ff' are displayed. A 'Delete' checkbox is checked. The entire interface is contained within a light gray box.

Static DNS

The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name `www.example.com` translates to the addresses `192.0.32.10` (IPv4).

Static DNS is a concept relative to Dynamic DNS, in static DNS system, the IP mapped is static without change.

You can map the specific IP to a user-friendly domain name. In LAN, you can map a PC to a domain name for convenient access. Or you can set some well known Internet IP mapping item so you're your router will respond quickly for your DNS query instead of querying for the ISP's DNS server.



The screenshot shows a web-based configuration interface. At the top, there is a blue header bar with the word 'Configuration' on the left. Below the header, there is a section titled 'Static DNS' with a small downward arrow icon. Underneath this, there is a sub-section titled 'Parameters'. Inside 'Parameters', there are two input fields: 'Host Name' and 'IP Address'. Below these fields are two buttons: 'Add' and 'Delete'. The 'Add' button is highlighted with a blue border, while the 'Delete' button is not.

Host Name: type the domain name for the specific IP.

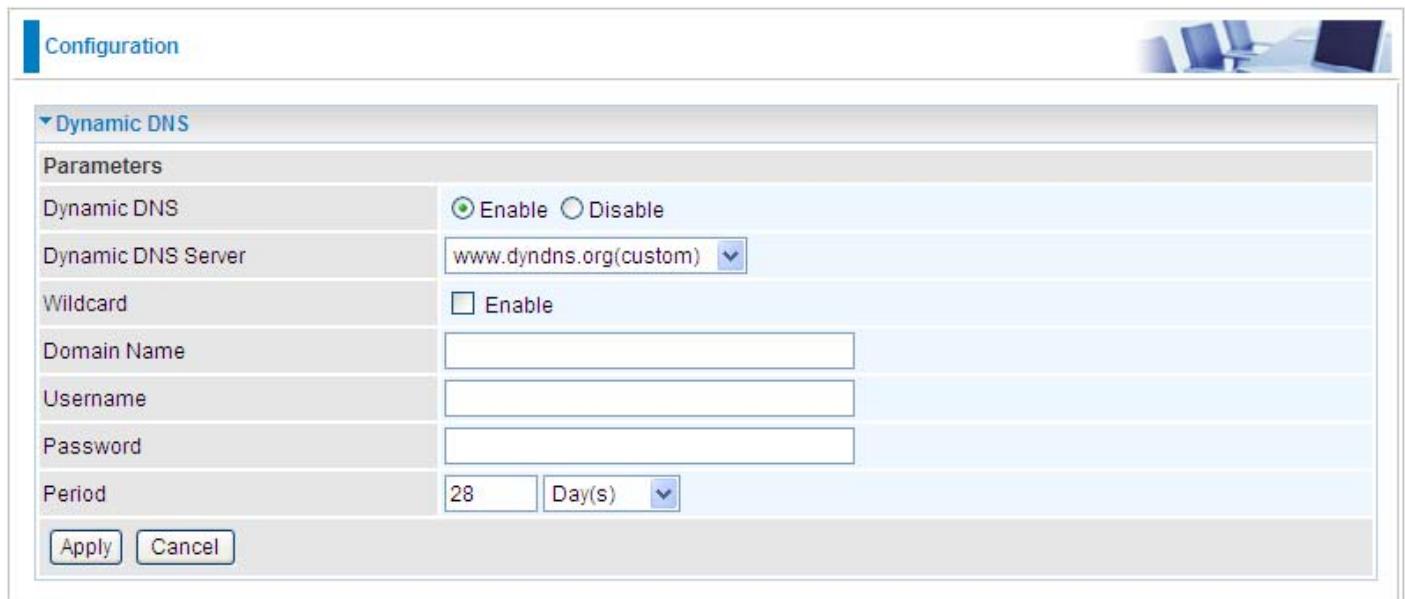
IP Address: type the IP address.

Click Add to add the static DNS item.

Dynamic DNS

The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still use a domain name. This is especially useful when hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than the dynamic IP address which is assigned to you by ISP.

You need to first register and establish an account with the Dynamic DNS provider using their website, for example <http://www.dyndns.org/>.



Configuration

Dynamic DNS

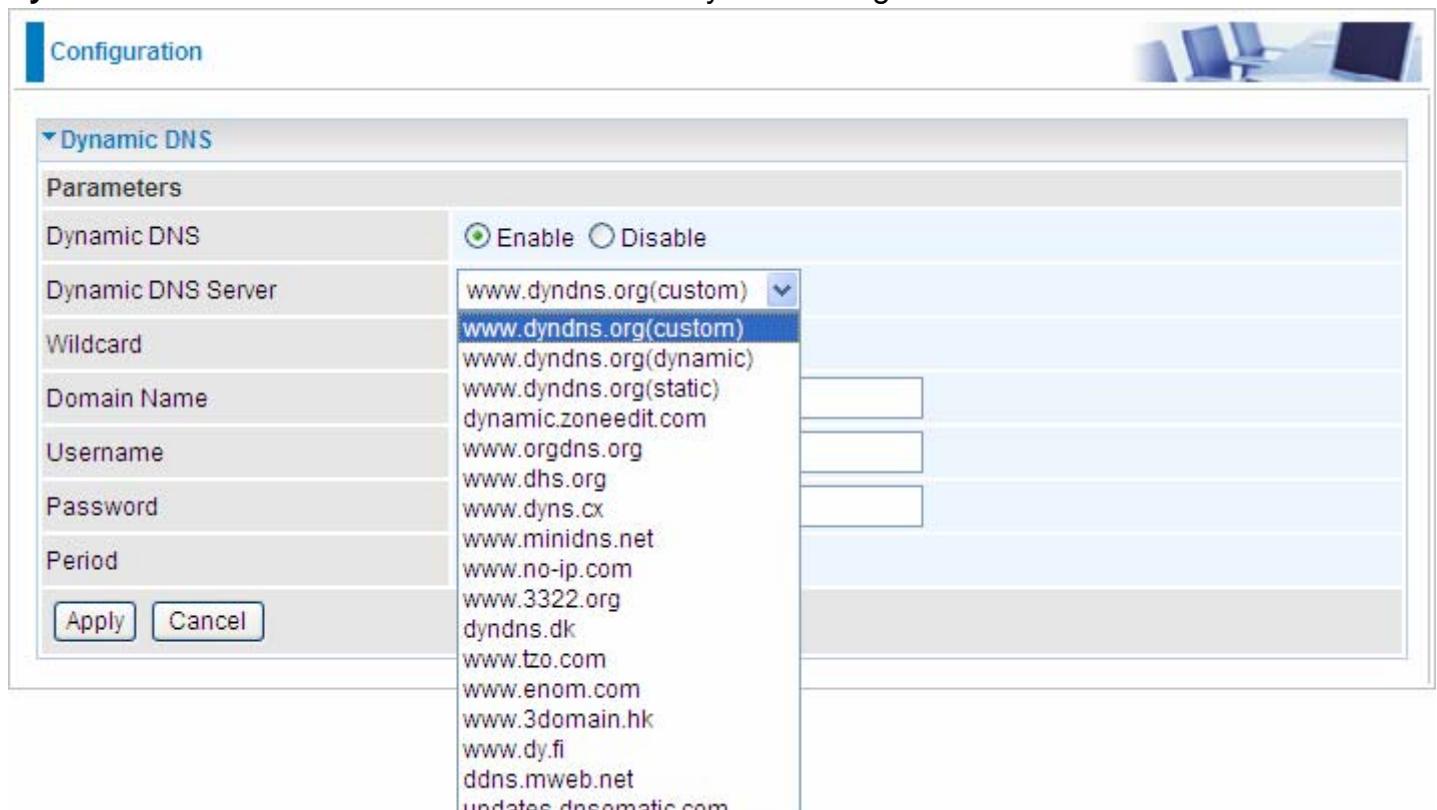
Parameters

Dynamic DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Dynamic DNS Server	www.dyndns.org(custom) <input type="button" value="▼"/>
Wildcard	<input type="checkbox"/> Enable
Domain Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Period	28 <input type="button" value="Day(s)"/> <input type="button" value="▼"/>

Apply Cancel

Dynamic DNS: Default is disabled. Check Enable to enable the Dynamic DNS function and the following fields will be activated and required.

Dynamic DNS Server: Select the DDNS service you have registered an account with.



Configuration

Dynamic DNS

Parameters

Dynamic DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Dynamic DNS Server	<input type="button" value="www.dyndns.org(custom)"/> <input type="button" value="▼"/>
Wildcard	<input type="checkbox"/>
Domain Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Period	<input type="text"/> <input type="button" value="Day(s)"/> <input type="button" value="▼"/>

Apply Cancel

www.dyndns.org(custom)
www.dyndns.org(custom)
www.dyndns.org(dynamic)
www.dyndns.org(static)
dynamic.zoneedit.com
www.orgdns.org
www.dhs.org
www.dyns.cx
www.minidns.net
www.no-ip.com
www.3322.org
dyndns.dk
www.tzo.com
www.enom.com
www.3domain.hk
www.dy.fi
ddns.mweb.net
updates.dnsomatic.com

Wildcard: When enabled, you allow the system to lookup on domain names that do not exist to have MX records synthesized for them.

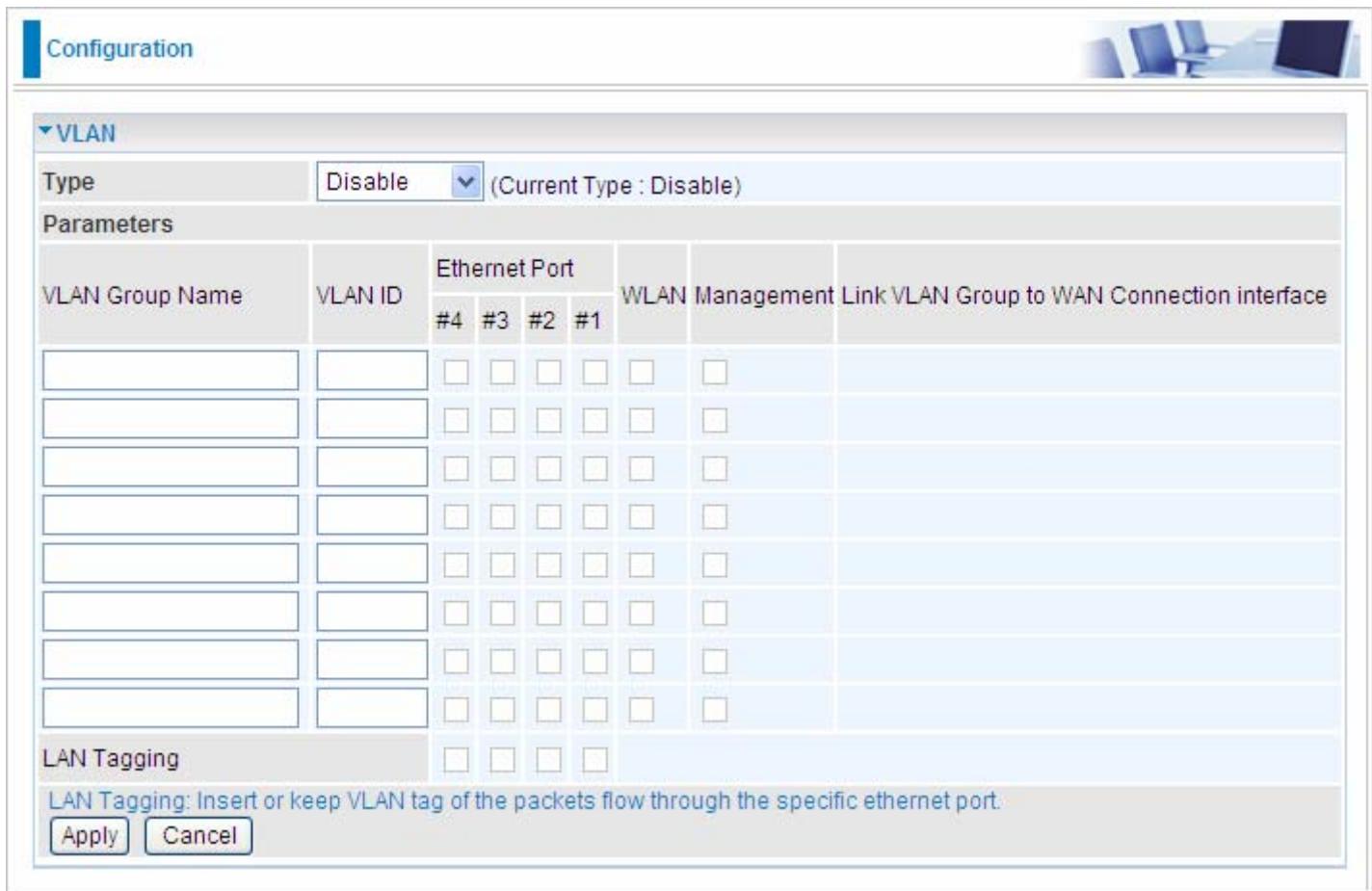
Domain Name, Username and Password: Enter your registered domain name and your username and password for this service.

Period: Enter the length of the period in the blank; you can set the period unit in day, hour or minute.

Click Apply to confirm the settings.

VLAN

VLAN (Virtual Local Area Network) is a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment.



The screenshot shows a configuration interface for VLAN settings. At the top, a blue bar contains the word "Configuration" and a small icon of three computer monitors. Below this is a section titled "VLAN" with a dropdown menu set to "Disable". The main area is a table for defining VLAN groups. The columns are: "VLAN Group Name", "VLAN ID", "Ethernet Port" (with sub-columns for ports #4, #3, #2, and #1), and "WLAN Management Link VLAN Group to WAN Connection interface". There are eight rows in the table, each with empty input fields. Below the table is a section for "LAN Tagging" with four checkboxes. A note below the table says "LAN Tagging: Insert or keep VLAN tag of the packets flow through the specific ethernet port." At the bottom are "Apply" and "Cancel" buttons.

Type: Select the VLAN type from the drop-down menu. There are two options: Tag Based and Disable.

Then enter the parameters in the fields of the table.

Click Apply to confirm the settings.

Example: IPTV Service Setting



This example is only to illustrate how to connect an Ethernet port to STB (Set Top Box) in a way to avoid IPTV traffic from affecting your home network. Nevertheless, the actual IPTV service setting still depends on the one offered by your local service provider.

Attention

Go to Advanced mode > Configuration > WAN > WAN Profile. Add a new WAN profile using the Pure Bridge protocol. Information should be provided by your local service provider.

Note: Description name should not contain any space.

Configuration

WAN Profile

Parameters

Profile Port: ADSL

Protocol: Pure Bridge

Description: IPTV

VPI / VCI: 0 / 35

Encap. method: LLC/SNAP-BRIDGING

When you finish configuring all WAN settings, please click the 'Restart' button for these changes to take effect.

Add Edit / Delete

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
<input type="radio"/>	PPPoE	ppp_0_8_35_1	0_8_35_2	8	35	LLC/SNAP-BRIDGING	Enable	0.0.0.0	<input type="checkbox"/>
<input checked="" type="radio"/>	Bridge	nas_0_0_35	IPTV	0	35	LLC/SNAP-BRIDGING	Disable		<input type="checkbox"/>

Then go to Advanced mode > Configuration > Advanced > VLAN. Then configure a port that will use the IPTV application. The example below is a setting that illustrates that only Ethernet port #4 can connect to STB and use IPTV.

Note: The VLAN setting illustrated bridges both WAN Profile and the Ethernet Port 4 so that the Ethernet port can connect to STB and get the IP directly from the IPTV Service Network. Thus, Ethernet port 4 can no longer be used for internet access and WEB management.

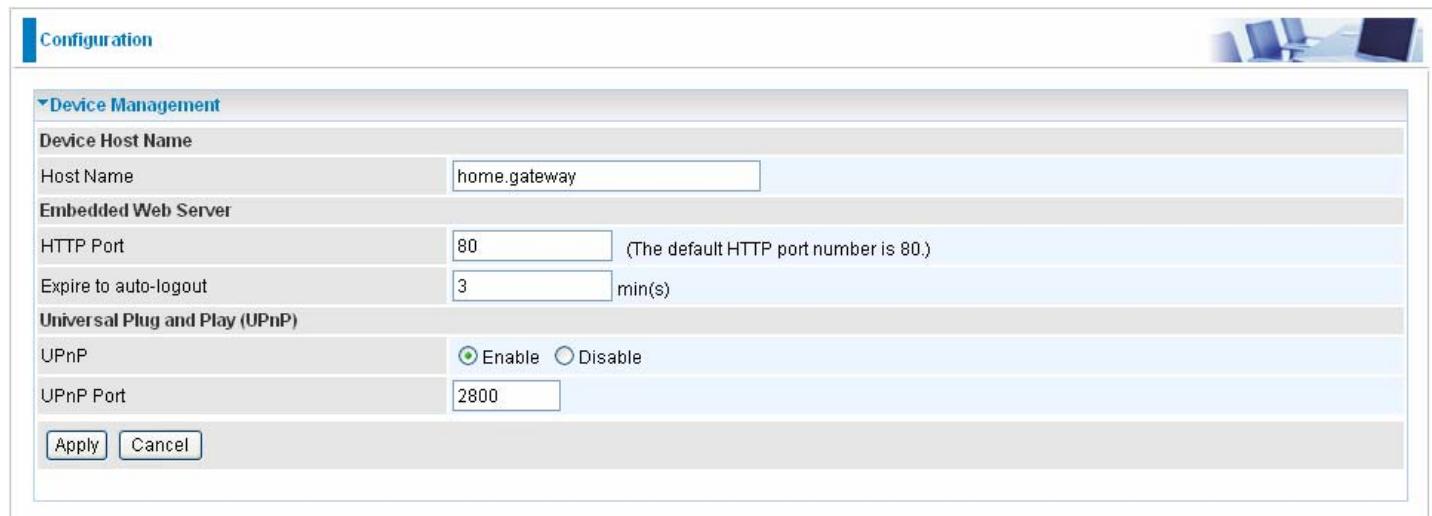
Configuration

VLAN

VLAN Group Name	VLAN ID	Ethernet Port				WLAN	Management	Link VLAN Group to WAN Connection	Interface
		#4	#3	#2	#1				
IPTV	2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	nas_0_0_35
Manage	3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	nas_0_0_35
		<input type="checkbox"/>	nas_0_0_35						
		<input type="checkbox"/>	nas_0_0_35						
		<input type="checkbox"/>	nas_0_0_35						
		<input type="checkbox"/>	nas_0_0_35						
		<input type="checkbox"/>	nas_0_0_35						
		<input type="checkbox"/>	nas_0_0_35						
		<input type="checkbox"/>	nas_0_0_35						
LAN Tagging		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
LAN Tagging: Insert or keep VLAN tag of the packets flow through the specific ethernet port.									
Apply	Cancel								

Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.



Device Management	
Device Host Name	
Host Name	home.gateway
Embedded Web Server	
HTTP Port	80 <small>(The default HTTP port number is 80.)</small>
Expire to auto-logout	3 min(s)
Universal Plug and Play (UPnP)	
UPnP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
UPnP Port	2800
Buttons	
Apply	Cancel

Device Host Name

Host Name: Assign it a name.

HTTP Port: The default HTTP port number is 80, you can change it to another one.

(The Host Name cannot be used with one word only. There are two words should be connected with a '.' at least.)

Example:

Host Name: homegateway => Incorrect

Host Name: home.gateway or my.home.gateway => Correct)

Expire to auto-logout: Specify a duration for the system to log the user out of the configuration session automatically.

Universal Plug and Play (UPnP)

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with the feature to control data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems. By letting the application control the required settings and removing the need for the user to control the advanced configuration of their device will make tasks such as port forwarding become easier.

Both user's Operating System and its relevant applications must support UPnP in addition to the router. Windows XP and Windows Me have a native built-in support for UPnP (when the component is installed). Windows 98 users may have to install the Internet Connection Sharing client from Windows XP in order to support UPnP feature. Windows 2000 does not support UPnP.

Disable: Check to deactivate the router's UPnP functionality.

Enable: Check to activate the router's UPnP functionality.

UPnP Port: Default setting is 2800. It is highly recommended for users to use this port value. If this value conflicts with other ports that have been used, you are allowed to change the port number.

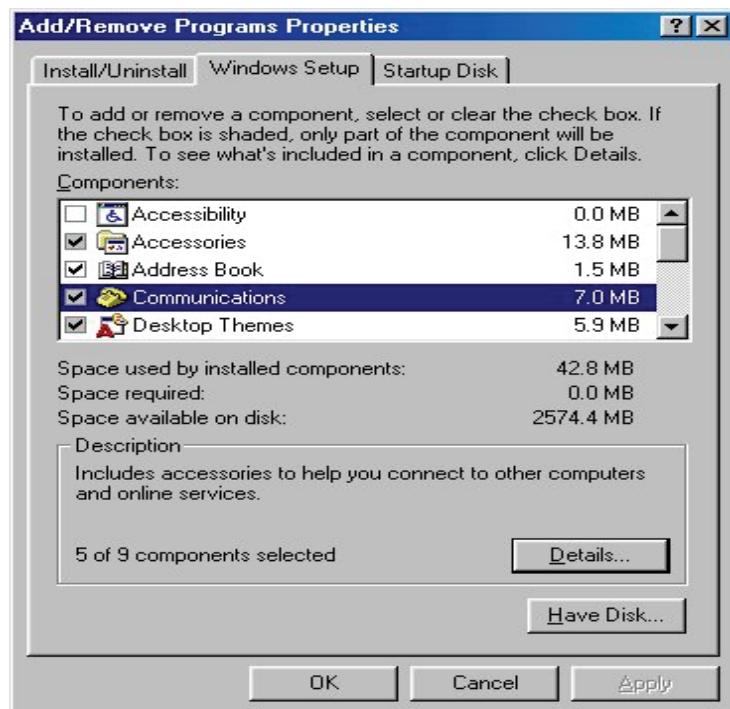
Click Apply to confirm the settings.

Installing UPnP in Windows Example

Follow the steps below to install the UPnP in Windows Me.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.



Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.



Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

Step 5: Restart the computer when prompted.

Follow the steps below to install the UPnP in Windows XP.

Step 1: Click Start and Control Panel.

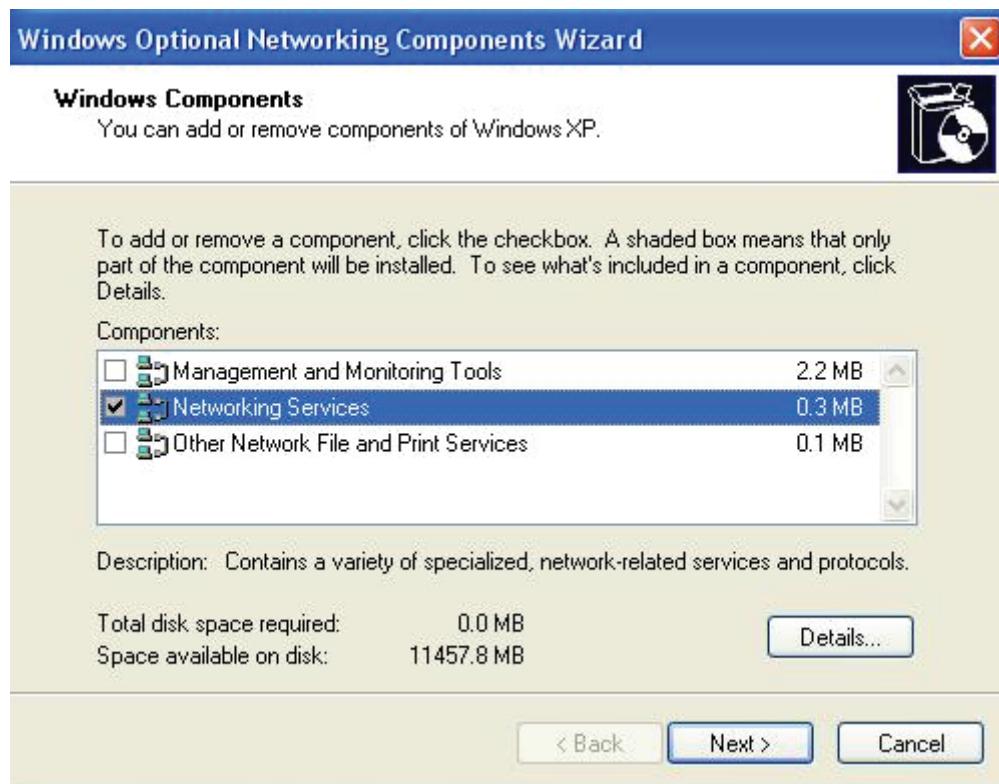
Step 2: Double-click Network Connections.

Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components

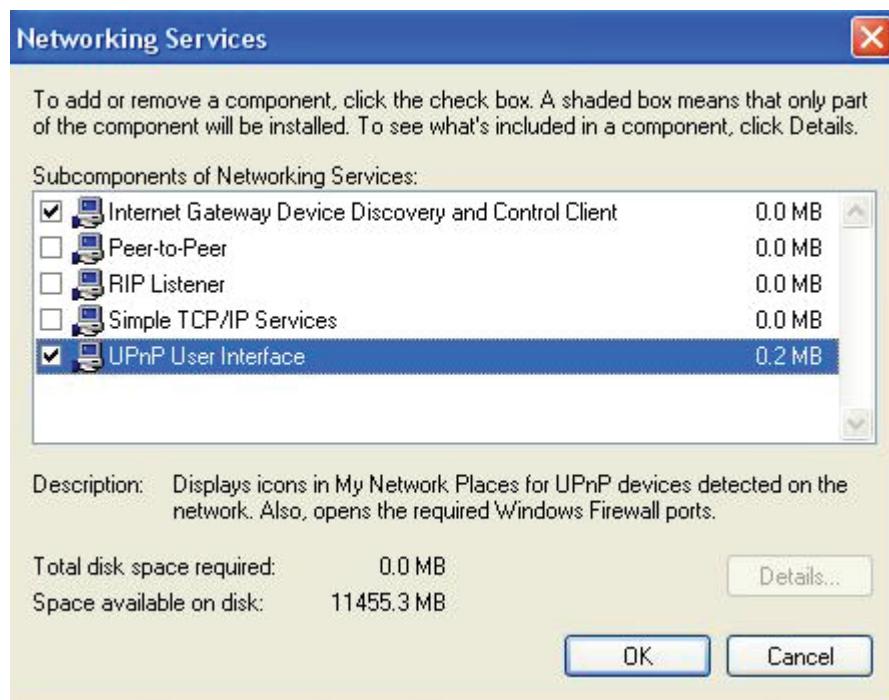
Step 4: When the Windows Optional Networking Components Wizard window appears, select Networking Service in the Components selection box and click Details.



Step 5: In the Networking Services window, select the Universal Plug and Play check box.



Step 6: Click OK to go back to the Windows Optional Networking Component Wizard window and click Next.



Auto-discover Your UPnP-enabled Network Device

Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

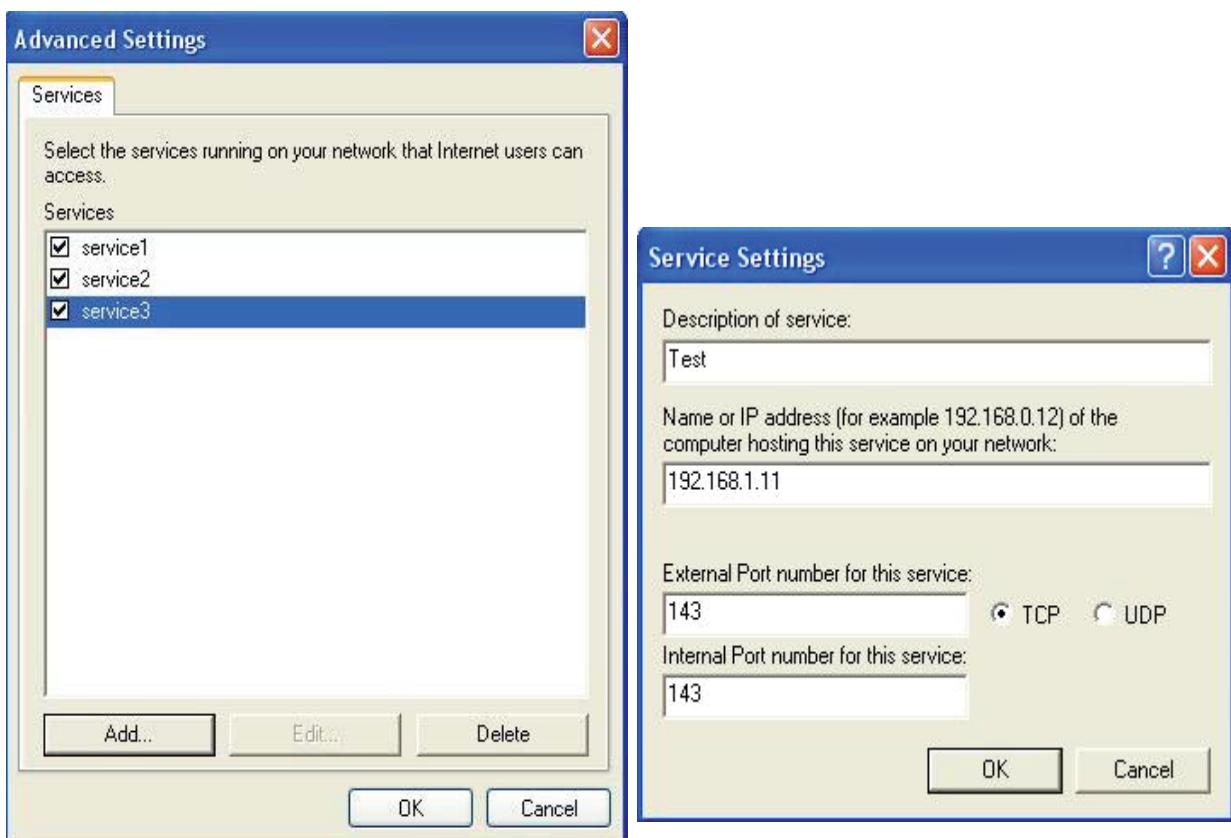
Step 2: Right-click the icon and select Properties.



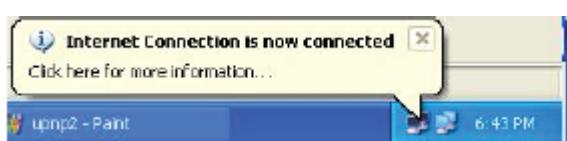
Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.



Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray.



Step 6: Double-click on the icon to display your current Internet connection status.



Web Configurator Easy Access

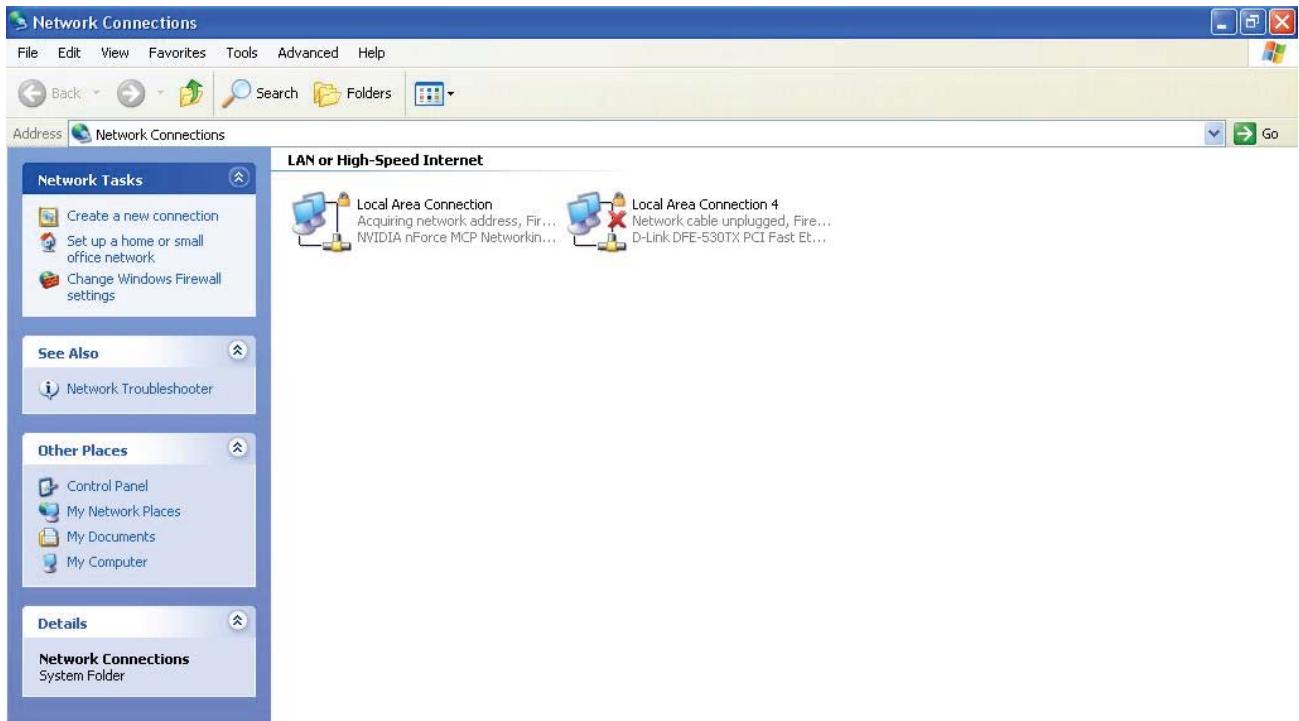
With UPnP, you can access web-based configuration for the BiPAC 7800GZ(L) without first finding out the IP address of the router. This helps if you do not know the router's IP address.

Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your BiPAC 7800GZ(L) and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BiPAC 7800GZ(L) and select Properties. A properties window displays basic information about the BiPAC 7800GZ(L).

IGMP

IGMP, known as Internet Group Management Protocol, is used to manage hosts from multicast group.



IGMP Proxy: IGMP proxy enables the system to issue IGMP host messages on behalf of the hosts that the system has discovered through standard IGMP interfaces. The system acts as a proxy for its hosts. Default is set to Disable.

IGMP Snooping: Allows a layer 2 switch to manage the transmission of any incoming IGMP multicast packet groups between the host and the router. Default is set to Disable.

Click Apply to confirm the settings.

Example:

When IGMP snooping is enabled, the feature will analyze all incoming IGMP packets between the hosts that are connected to the switch and the multicast routers in the network. When the layer 2 switch receives an IGMP report from a host requesting for a given multicast group, the switch will add the host's port number to the multicast list for that multicast group to be forwarded to. And, when the layer 2 switch has detected that an IGMP has left, it will remove the host's port from the table entry.

TR-069 Client

Please contact your ISP for the information of TR069.

Parameters	
Inform	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Inform Interval	300
ACS URL	
ACS Username	admin
ACS Password	*****
Connection Request Authentication	<input checked="" type="checkbox"/>
Connection Request Username	admin
Connection Request Password	*****

Apply **GetRPCMethods**

Inform: You may enable or disable the periodic inform feature.

Inform Interval: Enter the length of the periodic inform interval (unit: seconds).

ACS URL: Enter the ACS URL address.

ACS Username: Enter the ACS server login name.

ACS Password: Enter the ACS server login password.

Connection Request Authentication: Check to enable connection request authentication feature.

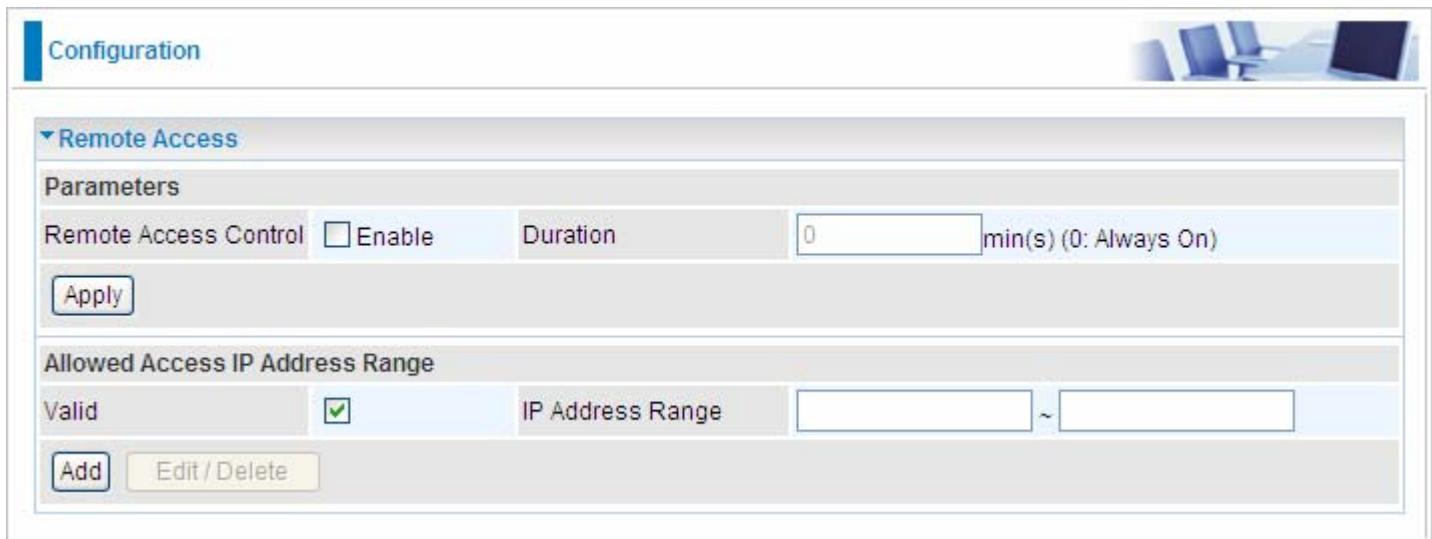
Connection Request Username: Enter the username for ACS server to make connection request.

Connection Request Password: Enter the password for ACS server to make connection request.

GetRPCMethods: Detect the types of methods that ACS supports and is in communication with.

Click Apply to confirm the settings.

Remote Access



The screenshot shows a configuration interface for 'Remote Access'. At the top, there is a 'Configuration' tab and a small icon of three computer monitors. The main section is titled 'Remote Access' with a 'Parameters' sub-section. It includes a checkbox for 'Remote Access Control' (checked), a 'Duration' field set to '0 min(s)' with '(0: Always On)' as an option. Below this is an 'Apply' button. The next section is 'Allowed Access IP Address Range', which has a 'Valid' checkbox checked. It includes fields for 'IP Address Range' with a start value of '192.168.1.100' and an end value of '192.168.1.150', separated by a tilde (~). There are 'Add' and 'Edit / Delete' buttons at the bottom of this section.

Remote Access Control: Select Enable to allow management access from remote side (mostly from internet).

"Allowed Access IP Address Range" was used to restrict which IP address could login to access system web GUI.

Valid: means to enable the IP address Range limitation.

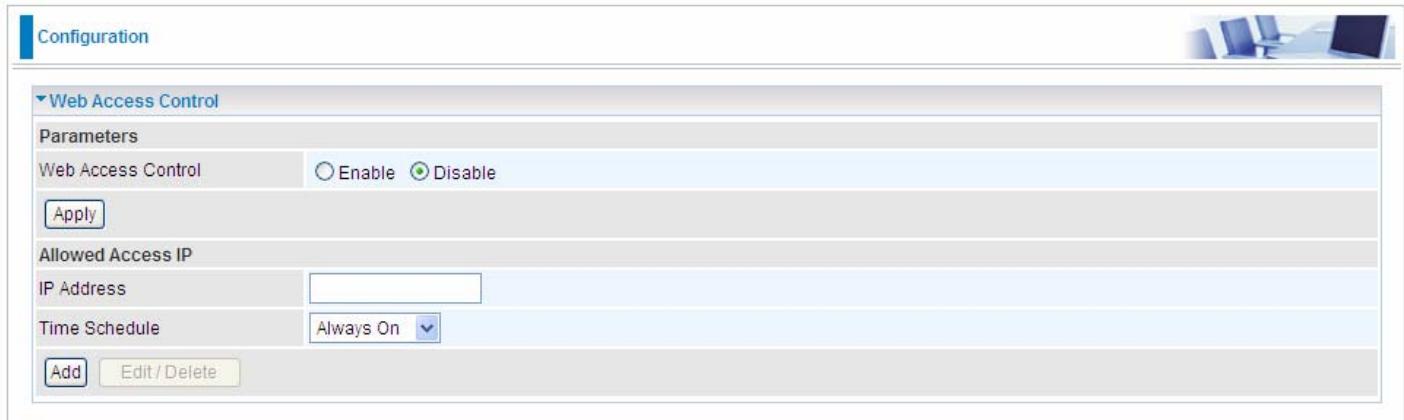
IP Address Range: specify the IP address Range.

Click **Apply** to confirm Remote Access Control setting.

Click **Add** to add an IP Range to allow remote access.

Web Access Control

Web access control is to only entitle authorized IPs to access the router's configuration webpage.



Configuration

Web Access Control

Parameters

Web Access Control Enable Disable

Apply

Allowed Access IP

IP Address:

Time Schedule: Always On

Add

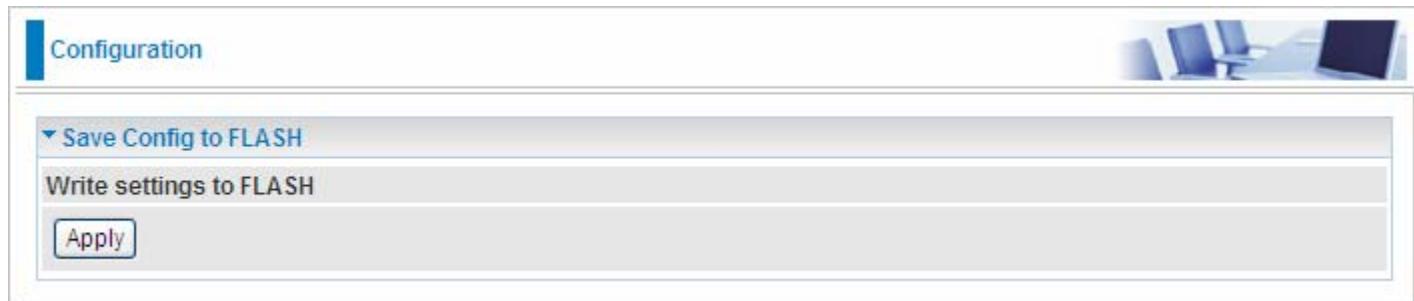
Web Access Control: Select “Enable” to allow the management of Web control.

Allowed Access IP: Enter the IP Address allowed.

Time Schedule: Choose the time scheduled for the setting.

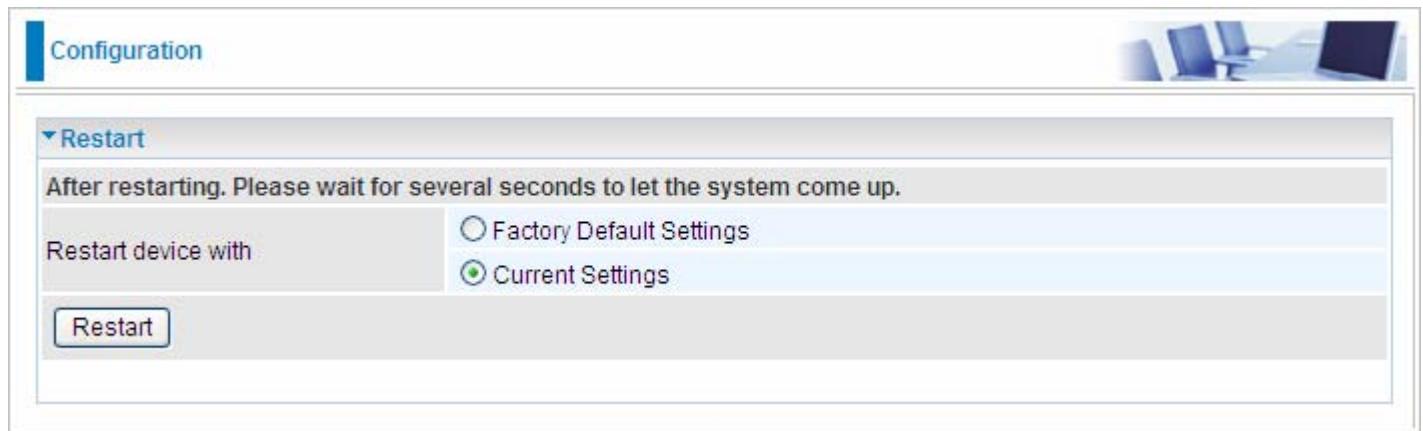
Save Configuration to Flash

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid losing them after turning off or resetting your router. Click "Save Config" and click "Apply" to write your new configuration to FLASH.



Restart

Click “Restart” with option Current Settings to reboot your router (and restore your last saved configuration).



If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings.

Logout

To exit the router web interface, choose Logout. Please save your configuration setting before logging out of the system.

Be aware that the router configuration interface can only be accessed by one PC at a time. Therefore when a PC has logged into the system interface, the other users cannot access the system interface until the current user has logged out of the system. If the previous user forgets to logout, the second PC can only access the router web interface after a user-defined auto logout period which is by default 3 minutes. You can however modify the value of the auto logout period using the Advanced > Device Management section of the router web interface. Please see the Advanced section of this manual for more information.

Chapter 5: Troubleshooting

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or Billion for support.

Problems with the router

Problem	Suggested Action
None of the LEDs lit when the router is turned on	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router more than 5 seconds.

Problems with WAN interface

Problem	Suggested Action
Frequent loss of ADSL linesync (disconnections)	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.
Either 3G or wireless performance is limited	Make sure you install the right antennae on the right jacks as mentioned in the package contents, hardware overview and hardware installation. If it remains occur, please refer to User manual or consult your service provider.

Problem with LAN interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

Appendix: Product Support & Contact

If you come across any problems please contact the dealer from where you purchased your product.

Contact Billion

Worldwide:

<http://www.billion.com>

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/98, Windows NT, Windows 2000, Windows Me, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.